

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK**

SHEILA LONG, MICHAEL DONIOS, JOSEPH
JONES JR., and MATTHEW SCHRIER,

Plaintiffs,

v.

MTN GROUP LIMITED, MTN IRANCELL, MTN
DUBAI LIMITED, ZTE CORPORATION, ZTE (USA)
INC., ZTE (TX) INC., HUAWEI TECHNOLOGIES
CO., LTD., HUAWEI TECHNOLOGIES USA INC.,
HUAWEI DEVICE USA INC., FUTUREWEI
TECHNOLOGIES, INC., and SKYCOM TECH CO.,
LTD.,

Defendants.

JURY TRIAL DEMANDED

Case No.: 23-cv-5705

**COMPLAINT FOR
VIOLATION OF THE ANTI-TERRORISM ACT**

Ryan R. Sparacino
Geoffrey P. Eaton
Eli J. Kay-Oliphant
Tejinder Singh
Shuman Sohrn
SPARACINO PLLC
1920 L Street, NW, Suite 835
Washington, DC 20036
Tel: 202.629.3530
ryan.sparacino@sparacinopllc.com
eli.kay-oliphant@sparacinopllc.com
geoff.eaton@sparacinopllc.com
tejinder.singh@sparacinopllc.com
shuman.sohrn@sparacinopllc.com

TABLE OF CONTENTS

	Page
A. THE MTN DEFENDANTS.....	18
B. THE ZTE DEFENDANTS	19
C. THE HUAWEI DEFENDANTS	20
I. SINCE THE ISLAMIC REVOLUTION IN 1979, THE ISLAMIC REVOLUTIONARY GUARD CORPS, OR IRGC, HAS FOMENTED AND SUSTAINED ANTI-AMERICAN TERRORISM	24
A. ISLAMIC REVOLUTIONARY GUARD CORPS	25
B. HEZBOLLAH.....	29
C. QODS FORCE.....	32
II. HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC LED A CONSPIRACY TO ACCOMPLISH THEIR “SECURITY” MISSION OF EXPELLING THE UNITED STATES FROM THE MIDDLE EAST.....	35
A. THE OBJECT OF THE CONSPIRACY AND ITS LEADERSHIP.....	35
B. THE PARTIES TO THE CONSPIRACY	38
1. FTO/SDGT Co-Conspirators	38
2. Corporate Front Co-Conspirators	39
i. MTN Irancell.....	39
ii. MTN Group.....	40
iii. TCI and MCI.....	42
iv. Exit40	42
3. Corporate Supplier and Manufacturer Co-Conspirators	43
C. PLAINTIFFS WERE INJURED BY ATTACKS IN AFGHANISTAN THAT OCCURRED IN FURTHERANCE OF THE CONSPIRACY	44
1. The Iraq/Syria Terror Campaign.....	44

2.	The Afghanistan Terror Campaign	45
III.	AFTER 9/11, HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, TALIBAN, AND AL-QAEDA JOINED AN IRGC CONSPIRACY TO DRIVE THE UNITED STATES OUT OF THE MIDDLE EAST.....	46
A.	THE FORMATION OF THE CONSPIRACY.....	46
1.	After 9/11, Hezbollah, The Qods Force, And Regular IRGC Led A Terrorist Conspiracy Targeting Americans In Afghanistan, Iraq, And Elsewhere To Inflict Pain On “The Great Satan”	46
2.	To Maximize The Lethality Of Their Terrorist Conspiracy, Hezbollah, The Qods Force, And Regular IRGC Provided Material Support To Every Other Member of the Conspiracy, Including Funds, Arms, Training, And Logistical Support, Which Their Co-Conspirators Used To Attack Americans in Afghanistan.....	46
B.	IN FURTHERANCE OF THE CONSPIRACY, HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, AL-QAEDA, THE TALIBAN, AND THE MEMBERS OF THE AL-QAEDA-TALIBAN TERRORIST SYNDICATE WAGED A DEADLY TERRORIST CAMPAIGN AGAINST AMERICANS IN AFGHANISTAN.....	49
1.	Al-Qaeda	53
2.	Sirajuddin Haqqani (Al-Qaeda and Taliban)	62
3.	The Taliban	66
4.	The Kabul Attack Network.....	72
C.	IN FURTHERANCE OF THE CONSPIRACY, THE IRGC, INCLUDING ITS HEZBOLLAH DIVISION AND QODS FORCE, AL-QAEDA, AL-QAEDA-IN-IRAQ, AND AL-NUSRA FRONT WAGED A DEADLY TERRORIST CAMPAIGN AGAINST AMERICANS IN IRAQ AND SYRIA.....	73
1.	Al-Qaeda	75
2.	Al-Qaeda-In-Iraq, Including Al-Nusra Front.....	79
3.	The IRGC’s, Including Its Hezbollah Division’s And Qods Force’s, Aid to Al-Qaeda, Al-Qaeda-in-Iraq, And Al-Nusra Front Facilitated Attacks Against Americans In Iraq in Syria, Including Plaintiff Matthew Schrier	82
i.	The IRGC, Including its Hezbollah Division and Qods Force, Provided Material Support and Resources to Sunni Terrorists Targeting	

Americans in Iraq, Including Al-Qaeda, Al-Qaeda-In-Iraq, and Ansar Al-Islam to Undermine the U.S. Mission There	85
ii. Iran Provided Material Support and Resources To Al-Qaeda That Established Al-Qaeda's Capabilities Before 9/11, Prevented Al-Qaeda's Collapse After 9/11, and Ensured Al-Qaeda's Status As An Iranian Sunni Terrorist Proxy in Iraq	87
iii. Iran Used the IRGC to Establish Al-Qaeda-In-Iraq as an Iranian Sunni Terrorist Proxy in Iraq	96
iv. Iran Used the IRGC to Establish Ansar Al-Islam as an Iranian Sunni Terrorist Proxy in Iraq	101
v. Iran Provided its Iraqi Sunni Terrorist Proxies with Weapons, Explosives, and Lethal Substances	104
vi. Iran Provided its Iraqi Sunni Terrorist Proxies with Lodging, Training, Expert Advice or Assistance, Safehouses, Personnel, and Transportation	108
vii. Iran Provided its Iraqi Sunni Terrorist Proxies with Financial Support.....	119
D. IN FURTHERANCE OF THE CONSPIRACY, HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC OPERATED AS AN INTEGRATED TRANSNATIONAL TERRORIST ORGANIZATION WITH A COMMON DOCTRINE, STRATEGY, FINANCIAL STRUCTURE, LOGISTICS STRUCTURE, AND COMMAND-AND-CONTROL	121
1. The IRGC's Transnational Terrorist Strategy, Doctrine, And Tactics Emphasize The Deployment Of Joint Cells Of Terrorists Led By Hezbollah, Funded And Resourced By The Qods Force, And Supported By Local Iranian Terrorist Proxies	121
2. Hezbollah, The Qods Force, And Regular IRGC Follow Common Terrorist Techniques, Tactics, And Procedures And Use The Same Terrorist Tradecraft To Ensure Concealment And Cover Worldwide.....	122
3. Hezbollah's, The Qods Force's, And Regular IRGC's Terrorist Tradecraft And Doctrine Has Historically Relied On Fronts, Operatives, Agents, Cut-Outs, And Orbits To Fund, Arm, And Operationally Aid IRGC Terrorist Proxy Attacks Against Americans	130
E. IN FURTHERANCE OF THE CONSPIRACY, HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC MANAGED A TRANSNATIONAL NETWORK OF TERRORIST FINANCE, LOGISTICS, OPERATIONS, AND COMMUNICATIONS CELLS TO FUND, ARM, LOGISTICALLY	

SUSTAIN, AND FACILITATE ATTACKS ON AMERICANS IN AFGHANISTAN	132
IV. THE CONSPIRACY DEPENDED UPON THE CO-CONSPIRATORS’ ROBUST ACCESS TO U.S. TECHNOLOGY, U.S. DOLLARS, AND U.S. PERSONS TO CARRY OUT ATTACKS AGAINST AMERICANS IN THE MIDDLE EAST	137
A. AFTER THE U.S. INVASIONS OF AFGHANISTAN AND IRAQ, HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC CONCLUDED THAT THEY NEEDED TO REVOLUTIONIZE THEIR ACCESS TO U.S. TECHNOLOGIES THROUGH CORRUPT CORPORATE PARTNERS	137
B. THE IRGC ADDRESSED THE CONSPIRACY’S FUNDING AND LOGISTICS NEEDS BY SEIZING IRAN’S LARGEST TELECOMMUNICATIONS COMPANIES TO ACQUIRE THE TECHNOLOGIES, CASH FLOW, AND LOGISTICAL AID FROM CORPORATE PARTNERS	144
1. MTN Irancell	145
2. Telecommunications Company Of Iran (TCI).....	147
V. DEFENDANTS FURTHERED THE CONSPIRACY AND TRANSACTED BUSINESS WITH FRONTS, OPERATIVES, AND AGENTS CONTROLLED BY HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC	148
A. THE BONYAD MOSTAZAFAN	148
B. IRAN ELECTRONICS INDUSTRIES	154
C. MTN IRANCELL	155
D. TELECOMMUNICATIONS COMPANY OF IRAN (TCI).....	157
E. THE AKBARI FRONT COMPANIES	159
F. EXIT40	160
VI. EACH DEFENDANT ENGAGED IN COMMERCIAL TRANSACTIONS THAT IT KNEW WERE STRUCTURED TO FINANCE, ARM, LOGISTICALLY AID, AND/OR OPERATIONALLY SUPPORT HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, AND THEIR TERRORIST PROXIES IN AFGHANISTAN	161
F. THE MTN DEFENDANTS.....	161

1.	MTN Group Joined The Conspiracy To Seize The “Virgin” Telecom Markets Controlled, Contested, Or Influenced By The IRGC And Its Terrorist Proxies.....	161
2.	MTN Group, MTN Dubai, And All MTN Subsidiaries And Affiliates Worldwide Joined The Terrorist Conspiracy.....	163
3.	MTN Knowingly Assumed A Financial, Logistical, And Operational Role In The IRGC’s, Including Hezbollah’s And The Qods Force’s, Sponsorship And Support Of Terrorist Attacks Against Americans Worldwide.....	178
4.	MTN Knowingly Assumed A Financial, Logistical, And Operational Role In The Taliban’s, Including The Haqqani Network’s, Terrorist Enterprise In Afghanistan, Directly And Indirectly Financing And Arming IRGC Proxy Attacks In Afghanistan And Iraq.....	192
	i. MTN Made Protection Payments To The Taliban.....	192
	ii. MTN Supported The Taliban By Deactivating Its Cellular Towers At Night	199
5.	MTN’s Assistance To Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, And The Taliban, Comports With MTN’s Historical Business Practices In International Markets	206
6.	MTN’s Acts In Furtherance Of The Conspiracy Had A Substantial Nexus To The United States	207
	i. MTN’s Conduct Targeted the United States.....	208
	ii. From 2012 Through 2019, MTN Group Regularly Reached Into The United States In Order To Unlock The U.S. Financial System So That MTN Group Could Repatriate Hundreds Of Millions Of Dollars Out Of MTN Irancell	211
	iii. MTN Group Facilitated A \$400,000 Bribe That Flowed Through The New York Financial System To A Cut-Out For The IRGC And Into The Budget Of Hezbollah, The Qods Force, And Regular IRGC	213
	iv. MTN Group And MTN Dubai Conspired To Provide, And Did Provide, A Stable, Robust, And Devastating Pipeline Of Illicitly Acquired State-of-the-Art American Technologies To Hezbollah, The Qods Force, And Regular IRGC, Including Untraceable American Smartphones.....	214
	v. MTN Obtained U.S. Technology For The Benefit Of Hezbollah, The Qods Force, And Regular IRGC	216

vi. MTN Obtained Essential U.S. Services That Aided Hezbollah's, the Qods Force's, and Regular IRGC's Terrorist Capabilities	217
G. THE ZTE DEFENDANTS	218
1. ZTE Joined The Terrorist Conspiracy	218
i. Through Agreements With Hezbollah, Qods Force, And Regular IRGC Fronts Including But Not Limited To MTN Irancell, TCI, and Exit40, ZTE Agreed To Join A Company-Wide Conspiracy	218
ii. ZTE, ZTE USA, And ZTE TX Each Made Overt Acts In Furtherance Of The Conspiracy	219
2. ZTE Knowingly Assumed A Financial, Logistical, And Operational Role In Hezbollah's, The Qods Force's, And Regular IRGC's Terrorist Enterprise Against Americans Worldwide	219
i. ZTE Corp., ZTE USA, And ZTE TX Knowingly Facilitated MTN Irancell And TCI's Acquisition Of Embargoed American Technology, Logistical Support, And Technical Services, Which Flowed Through To The IRGC's Terrorist Proxies	220
ii. ZTE Corp., ZTE USA, And ZTE TX Substantially Increased MTN Irancell And TCI Revenue By Illicitly Sourcing Embargoed American Technology, Logistical Support, And Technical Services, Which Flowed Through To The IRGC's Terrorist Proxies	230
iii. ZTE Corp., ZTE USA, And ZTE TX Routed Bribes To The Key Procurement Decisionmakers At MTN Irancell And TCI, Which Flowed Through To The IRGC's Terrorist Proxies	231
3. ZTE Knowingly Assumed A Financial, Logistical, And Operational Role In The Taliban's, Including The Haqqani Network's, Terrorist Enterprise In Afghanistan, Directly And Indirectly Financing And Arming IRGC Proxy Attacks In Afghanistan And Iraq	234
4. ZTE's Assistance To Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, And The Taliban, Comports With ZTE's Historical Business Practices In International Markets	240
5. ZTE's Assistance To Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, And The Taliban Had A Substantial Nexus To The U.S.	242
i. ZTE's Conduct Targeted the United States	243
ii. ZTE's Conduct Relied on American Contacts	251

H.	THE HUAWEI DEFENDANTS	253
1.	Huawei Joined The Terrorist Conspiracy	253
	i. Through Agreements With Hezbollah, Qods Force, And Regular IRGC Fronts, Including But Not Limited to TCI And Exit40, Huawei Agreed To Join A Company-Wide Conspiracy	253
	ii. Huawei Co., Huawei USA, Huawei Device USA, Futurewei, And Skycom Each Made Overt Acts In Furtherance Of The Conspiracy	254
2.	Huawei Knowingly Assumed A Financial, Logistical, And Operational Role In The IRGC's, Including its Hezbollah Division's And Qods Force's, Terrorist Enterprise Against Americans Worldwide	255
	i. Huawei Co., Huawei USA, Huawei Device USA, Futurewei, And Skycom Knowingly Facilitated MTN Irancell And TCI Acquisition of Embargoed American Technology, Logistical Support, And Technical Services, Which Flowed Through To The IRGC's Terrorist Proxies	255
	ii. Huawei Substantially Increased MTN Irancell And TCI Revenue By Illicitly Sourcing Embargoed U.S. Technology, Which Flowed Through To The IRGC's Terrorist Proxies	269
	iii. Huawei Routed Bribes To The Key Procurement Decisionmakers At MTN Irancell And TCI, Which Flowed Through To The IRGC's Terrorist Proxies.....	269
	iv. The Huawei Defendants Routed "Free Goods" To The Key Procurement Decisionmakers At MTN Irancell And TCI, Which Flowed Through To The IRGC's Terrorist Proxies.....	270
3.	Huawei Knowingly Assumed A Financial, Logistical, And Operational Role In The Taliban's, Including The Haqqani Network's, Terrorist Enterprise In Afghanistan, Directly And Indirectly Financing And Arming IRGC Proxy Attacks In Afghanistan And Iraq	271
4.	Huawei's Assistance To Hezbollah, The Qods Force, Regular IRGC, Al- Qaeda, And The Taliban, Comports With Huawei's Historical Business Practices In International Markets	277
5.	Huawei's Assistance To Hezbollah, The Qods Force, Regular IRGC, Al- Qaeda, And The Taliban Had A Substantial Nexus To The United States	279
	i. Huawei's Conduct Targeted the United States	279
	ii. Huawei's Conduct Relied on American Contacts.....	283

VII.	DEFENDANTS’ TRANSACTIONS WITH FRONTS, OPERATIVES, AND AGENTS OF HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, AL-QAEDA, AND THE TALIBAN CAUSED FUNDS, ARMS, LOGISTICAL AID, AND OPERATIONAL SUPPORT TO FLOW THROUGH TO AL-QAEDA AND TALIBAN TERRORISTS AND AIDED THEIR ATTACKS AGAINST AMERICANS IN AFGHANISTAN	286
A.	HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC SOURCED WEAPONS, RAISED FUNDS, AND OBTAINED LOGISTICAL AND OPERATIONAL SUPPORT THROUGH ILLICIT CORPORATE TRANSACTIONS IN THE TELECOM, COMMUNICATIONS, AND IT SECTORS	286
B.	DEFENDANTS MADE ILLICIT DEALS WITH HEZBOLLAH, QODS FORCE, AND REGULAR IRGC FRONTS, OPERATIVES, AGENTS, AND CUT-OUTS THAT CAUSED SECURE AMERICAN SMARTPHONES, ENTERPRISE LEVEL SERVERS, NETWORK COMPUTING TECHNOLOGIES, AND WEAPONS TO FLOW THROUGH THE IRGC TO AL-QAEDA AND THE TALIBAN AND FACILITATE TERRORIST ATTACKS ON AMERICANS IN AFGHANISTAN	289
C.	DEFENDANTS MADE ILLICIT DEALS WITH HEZBOLLAH, QODS FORCE, AND REGULAR IRGC FRONTS, OPERATIVES, AGENTS, AND CUT-OUTS THAT CAUSED SUBSTANTIAL FUNDS TO FLOW THROUGH THE IRGC TO AL-QAEDA AND THE TALIBAN AND FACILITATED TERRORIST ATTACKS AGAINST AMERICANS IN AFGHANISTAN	292
1.	Procurement Bribery	292
2.	“Free Goods”	294
3.	Exit40	296
i.	Exit40 Was An IRGC Front	296
i.	MTN Group Knowingly Used Exit40 To Finance Hezbollah And The Qods Force	297
ii.	ZTE Corp. Knowingly Used Exit40 To Finance Hezbollah And The Qods Force	299
iii.	Huawei Co. Knowingly Used Exit40 To Finance Hezbollah And The Qods Force	300
D.	DEFENDANTS’ PROTECTION PAYMENTS TO THE TALIBAN DIRECTLY AIDED TERRORIST ATTACKS ON AMERICANS IN AFGHANISTAN	301

1.	Defendants’ Cash Protection Payments To The Taliban Directly Funded Al-Qaeda And Taliban, Including Haqqani Network, Attacks Against Americans In Afghanistan	303
2.	Defendants’ “Free Goods” Protection Payments To The Taliban Directly Funded, Armed, And Logistically Supported Al-Qaeda And Taliban, Including Haqqani Network, Attacks Against Americans In Afghanistan.....	308
VIII.	DEFENDANTS KNEW THAT THEIR TRANSACTIONS WITH HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, AL-QAEDA, AND THE TALIBAN FACILITATED EVERY NODE OF THE CONSPIRACY AND DIRECTLY AIDED TERRORIST ATTACKS AGAINST AMERICANS IN AFGHANISTAN	314
A.	DEFENDANTS KNEW THEIR TRANSACTIONS WITH HEZBOLLAH, QODS FORCE, AND REGULAR IRGC FRONTS, OPERATIVES, AGENTS, AND CUT-OUTS FURTHERED THE IRGC’S CONSPIRACY TO ATTACK AMERICANS IN AFGHANISTAN.....	314
1.	Command, Control, Communications, And Intelligence.....	330
2.	Terrorist Finance	332
3.	Weapons.....	337
2.	Recruiting, Fundraising, Strategic Communications, And Disinformation.....	340
B.	DEFENDANTS KNEW THAT THEIR PROVISION OF “SECURITY” “COOPERATION” AID TO HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC SUPPORTED TERRORIST ATTACKS AGAINST AMERICANS IN AFGHANISTAN BY IRGC PROXIES AL-QAEDA AND THE TALIBAN BECAUSE DEFENDANTS KNEW THAT “SECURITY” WAS AN IRGC EUPHEMISM FOR THE IRGC PROXY ATTACKS AGAINST AMERICANS	349
1.	In-Person IRGC Communications as Terrorist Tradecraft	349
2.	Iranian Constitution	350
3.	Iranian National Security Council	350
4.	Hezbollah Structure	351
5.	IRGC Doctrine	351
6.	Iran-Focused Scholars.....	352
7.	Terrorist Statements	353

8.	Iran-Related “Security” Media Coverage	354
9.	“Security” Euphemism-Related Media Coverage	356
10.	Each Defendant’s Consciousness of Guilt.....	358
C.	DEFENDANTS KNEW THEIR ILLICIT TRANSFERS OF CELL PHONES TO HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC AIDED THE CONSPIRACY’S TERRORIST ATTACKS AGAINST AMERICANS WORLDWIDE	360
D.	DEFENDANTS KNEW THAT THEIR PROTECTION PAYMENTS TO THE TALIBAN, FACILITATED TERRORIST ATTACKS BY AL-QAEDA AND THE TALIBAN AGAINST AMERICANS IN AFGHANISTAN AND WERE OPPOSED BY THE U.S. GOVERNMENT FOR THAT REASON.....	362
1.	Defendants Knew That Their Cash And “Free Goods” Protection Payments To The Taliban, Financed, Armed, And Logistically Sustained Terrorist Attacks By Al-Qaeda And The Taliban Against Americans In Afghanistan.....	362
2.	Defendants Knew That The U.S. Government Opposed Defendants’ Payment Of Protection Money To The Taliban.....	371
IX.	DEFENDANTS’ FINANCIAL, LOGISTICAL, AND OPERATIONAL AID TO THE IRGC AND PROTECTION PAYMENTS TO THE TALIBAN FLOWED THROUGH TO FACILITATE TERRORIST ATTACKS AGAINST AMERICANS IN AFGHANISTAN THAT WERE PLANNED, AUTHORIZED, AND OFTEN JOINTLY COMMITTED BY AL-QAEDA	375
A.	IN FURTHERANCE OF THE IRGC CONSPIRACY, THE IRGC RELIED UPON DEFENDANTS’ RESOURCES TO PROVIDE KEY ASSISTANCE TO AL-QAEDA AND THE TALIBAN, THAT FACILITATED TERRORIST ATTACKS AGAINST AMERICANS IN AFGHANISTAN IN ORDER TO DRIVE THE UNITED STATES OUT OF AFGHANISTAN IN FURTHERANCE OF THE IRGC’S CONSPIRACY	375
1.	The IRGC, Including Its Hezbollah Division And Qods Force, Provided Material Support For Anti-American Terrorism In Afghanistan To Undermine The U.S. Mission There.....	376
2.	The IRGC, Including Its Hezbollah Division And Qods Force, Provided The Taliban, With Weapons, Explosives, And Lethal Substances.....	383
3.	The IRGC, Including Its Hezbollah Division And Qods Force, Provided The Taliban With Lodging, Training, Expert Advice Or Assistance, Safehouses, Personnel, And Transportation	384

4.	The IRGC, Including Its Hezbollah Division And Qods Force, Provided The Taliban With Financial Support.....	385
5.	The IRGC, Including Its Hezbollah Division And Qods Force, Provided Material Support to Al-Qaeda to Facilitate Syndicate Attacks in Afghanistan.....	386
B.	IN FURTHERANCE OF THE IRGC CONSPIRACY, AL-QAEDA AUTHORIZED AND PLANNED THE ATTACKS THAT INJURED PLAINTIFFS	392
1.	Al-Qaeda Authorized the Attacks that Injured Plaintiffs.....	392
2.	Al-Qaeda Planned the Attacks that Injured Plaintiffs.....	394
C.	IN FURTHERANCE OF THE IRGC CONSPIRACY, AL-QAEDA COMMITTED TERRORIST ATTACKS THAT KILLED AND INJURED PLAINTIFFS IN JOINT CELLS WITH THE TALIBAN, LASHKAR-E-TAIBA, AND JAISH-E-MOHAMMED	397
X.	THE IRGC-BACKED TALIBAN TERRORIST SYNDICATE IN AFGHANISTAN AND PAKISTAN LED BY AL-QAEDA AND THE TALIBAN KILLED AND INJURED PLAINTIFFS THROUGH TERRORIST ATTACKS FOR WHICH DEFENDANTS PROVIDED SUBSTANTIAL ASSISTANCE	400
A.	AUGUST 20, 2013 SMALL ARMS ATTACK IN WARDAK (GEORGE BANNAR JR.)	402
B.	JANUARY 20, 2014 SMALL ARMS ATTACK IN KANDAHAR (EDWARD BALLI).....	403
C.	JUNE 2, 2014 SMALL ARMS ATTACK IN NANGARHAR (JASON JONES)	403
XI.	THE IRGC’S TERRORIST PROXIES COMMITTED, PLANNED, AND AUTHORIZED THE ATTACK THAT INJURED PLAINTIFF MATTHEW SCHRIER IN SYRIA	404
	COUNT ONE	398
	COUNT TWO	402
	COUNT THREE	406

RELATEDNESS

Plaintiffs believe that this matter is substantially similar to *Zobay et al. v. MTN Group Ltd. et al.*, Case 1:21-cv-03503 (E.D.N.Y. Compl. filed June 22, 2021) (Amon, J.) and *Lau et al. v. ZTE Corp., et al.*, Case 1:22-cv-01855 (E.D.N.Y. Compl. filed Apr. 3, 2022) (Amon, J.), and Plaintiffs have designated this matter as related to both. For the Court's benefit, Plaintiffs have appended to this Complaint as **Exhibit B** a redline showing the differences between this Complaint and the First Amended Complaint filed in *Lau* on August 22, 2022.

INTRODUCTION

1. This lawsuit seeks damages under the federal Anti-Terrorism Act (the "ATA") on behalf of family members of three American service members whose loved ones were killed while serving their country in Afghanistan between 2013 and 2014 (the "Afghanistan Plaintiffs"), and one American photojournalist who was abducted in Aleppo, Syria in late 2012, and brutally tortured and held hostage for more than 200 days until his escape in 2013. Plaintiffs seek to hold MTN, a South African telecom company, and ZTE and Huawei, two Chinese telecom companies and technology manufacturers, accountable for their conspiracy with, and substantial assistance to, multiple Foreign Terrorist Organizations ("FTOs") targeting Americans in the Middle East, including Syria, Afghanistan and Iraq.

2. Plaintiffs' allegations are based on information derived from confidential witnesses with direct and indirect knowledge of the alleged facts, internal company documents, declassified military intelligence reporting, congressional testimony and reports, press accounts, and Plaintiffs' recollections.

3. MTN, ZTE, and Huawei are large multinational companies that had lucrative business in Iran and Afghanistan that relied upon regular transactions with counterparties that MTN, ZTE, and Huawei knew served as fronts for terrorist finance and logistics, and MTN,

ZTE, and Huawei engaged in illicit, terrorism-sanctions-busting transactions with known terrorist fronts in order to boost their profits. Those transactions aided and abetted terrorism by directly funding, arming, and logistically supporting a terrorist campaign that stretched for nearly two decades, killing and injuring thousands of Americans.

4. MTN, ZTE, and Huawei provided two separate streams of devastating aid that ultimately flowed to benefit al-Qaeda (including its Iraqi and Syrian branches, al-Qaeda-in-Iraq ("AQI") and al-Nusra Front ("ANF")) and Taliban terrorists who killed and injured Plaintiffs or their loved ones in attacks from 2012 through 2014.

5. *First*, MTN, ZTE, and Huawei directly provided funding, technology, weapons, services, and other aid to the world's worst sponsor of terrorism, Iran's Islamic Revolutionary Guards Corps (or "IRGC"), including its Lebanese Hezbollah Division and Qods Force, in furtherance of the IRGC's conspiracy to target and kill Americans in the Middle East, including Afghanistan, in order to drive the United States from the region. The IRGC relied upon such aid to facilitate attacks by its proxies in Afghanistan, al-Qaeda and the Taliban, both of whom joined the IRGC's conspiracy to expel the United States from the countries on Iran's borders, Afghanistan and Iraq. Such aid flowed through the IRGC, including through Hezbollah and the Qods Force, and reached al-Qaeda and the Taliban, who deployed the IRGC's aid to sustain a successful nearly two-decades-long terrorist campaign against Americans there. Such aid went directly to AQI and its Syrian progeny, ANF.

6. *Second*, MTN, ZTE, and Huawei made substantial protection payments, in cash and "free goods," to the Taliban, including its Haqqani Network,¹ to further the IRGC's

¹ The Haqqani Network has always been, and remains, a part of the Taliban. In this Complaint, all references to "Taliban" include the Haqqani Network.

conspiracy and redirect violence away from MTN's, ZTE's, and Huawei's shipments, facilities, and projects in Afghanistan. MTN's, ZTE's and Huawei's protection payments to the Taliban provided an equally potent stream of aid to the terrorists, directly funding, arming, and logistically sustaining the Taliban.

7. This case reveals conduct that is unusually depraved. Few ATA defendants have ever been credibly accused of the full spectrum of behavior identified in this Complaint against MTN, ZTE, and Huawei, each of whom directly conspired with known fronts for designated terrorist organizations. In serving as full-spectrum telecommunications and computing partners for Hezbollah, the Qods Force, and Regular IRGC and, through these IRGC components, for long-standing IRGC proxies like al-Qaeda and the Taliban, MTN, ZTE, and Huawei aided *every* facet of the IRGC's terrorist enterprise and the broader IRGC Conspiracy that it served. Moreover, by making protection payments to the Taliban, MTN, ZTE, and Huawei provided a second equally potent stream of value that also provided cross-cutting financial, logistical, and operational benefits to the terrorists who committed the attacks that injured Plaintiffs and their loved ones.

8. MTN, ZTE, and Huawei aided the terrorists because they were co-conspirators with the IRGC, as each signed written agreements pledging to support the "security" agenda of their counterparty "Iranian Shareholders" – which were themselves fronts for the IRGC – which they and the IRGC both knew meant supporting the IRGC's, including Hezbollah's and the Qods Force's, industrial-scale exportation of terror targeting Americans worldwide, including in Syria and Afghanistan.

9. Here's how the Conspiracy worked: the IRGC led a conspiracy, the object of which was to commit terrorist attacks on Americans in the countries bordering Iran, Afghanistan

and Iraq and drive the U.S. out of the Middle East (the “IRGC Conspiracy” or “Conspiracy”). The IRGC established the IRGC Conspiracy after 9/11 and it continues even after the end of the conflict in Afghanistan. The co-conspirators along with the IRGC in the IRGC Conspiracy included terrorist groups integral to or supported by the IRGC, including its Hezbollah Division and Qods Force, al-Qaeda, the Taliban, and others. Corporate fronts for the IRGC, including the telecom companies the IRGC controlled such as MTN Irancell, the Telecommunications Company of Iran (“TCI”), and Mobile Communication Company of Iran (“MCI”) were also co-conspirators. The IRGC Conspiracy operated through its terrorist members to carry out attacks on Americans, with the IRGC providing logistical and financial support. The attacks in this case were all acts in furtherance of the IRGC Conspiracy. Every person and entity that agreed to join the IRGC Conspiracy is therefore liable for the harm caused by these attacks.

10. MTN, ZTE, and Huawei joined the IRGC Conspiracy on the dates they agreed with known IRGC fronts (variously, MTN Irancell, TCI, and MCI) to provide resources, technical materials, and technical support, and to support Iran’s “security” objectives.

11. Each of MTN, ZTE, and Huawei acted in furtherance of that agreement to join the IRGC Conspiracy each time they provided money and other resources, provided technical goods, such as cell phones and telecom infrastructure, assisted with technical support, as was their obligation as joint venturers with and contractual counterparties to known IRGC fronts, when they evaded U.S. sanctions in order to do so, and when they attempted to obfuscate their respective roles. Each time MTN, ZTE, and Huawei did these acts in furtherance of the IRGC Conspiracy, such person assisted the IRGC Conspiracy’s objective to attack Americans and furthered the IRGC Conspiracy’s ultimate objective to expel the U.S. from Afghanistan and Iraq.

12. MTN, ZTE, and Huawei entered into the IRGC Conspiracy with the IRGC, and acted in furtherance thereof for well over a decade. MTN, ZTE, and Huawei were one in spirit with their IRGC terrorist partners because each calculated that, if they remained aligned with the “Iranian Shareholders” – fronts for the IRGC – their company would reap billions in profits by seizing a monopoly in one of the world’s fastest-growing and youngest potential subscriber pools.

13. To earn their billions, MTN, ZTE, and Huawei simply needed to believe that the obvious and vast American bloodshed in Afghanistan and Iraq that was sure to follow their decision was an acceptable price to pay to yield a profitable outcome for their own shareholders and the “Iranian Shareholders” with whom they were at times joint venture partners and at others explicit contractual counterparties. Seasoned investors, however, know that for every shareholder who wins, another must lose. But this is not a case about trading shares on the NASDAQ. Here, the “shareholders” who lost were not day traders who got crushed making an unwise stock pick. They were the Plaintiffs: patriotic American servicemembers and civilians who volunteered for hard, thankless, jobs on the other side of the world in Afghanistan. Some returned, badly injured. Some never came back at all. None will ever be the same again. MTN, ZTE, and Huawei played a key role in the events that led to this outcome. Plaintiffs are among the victims. This lawsuit followed.

14. It is impossible to overstate the magnitude of MTN’s, ZTE’s, and Huawei’s defilement of the Anti-Terrorism Act. This case concerns one of the single most depraved, expansive, deceitful, and persistent international corporate conspiracies since the end of World War II, led by the IRGC and enabled by their corporate co-conspirators, MTN, ZTE, and Huawei. There is little doubt that the IRGC Conspiracy changed the trajectory of Afghanistan,

Iraq, and countless other countries. This Complaint outlines the unprecedented nature of MTN's, ZTE's, and Huawei's conduct, and it likely remains the tip of the iceberg. Few other defendants in the history of the ATA have engaged in conduct as comprehensively violative, for more money, over a longer period, with a more violent counterparty, with more devastating consequences, while demonstrating a greater sense of corporate impunity. For more than a decade, MTN, ZTE, and Huawei funded, partnered with, and helped develop the technical capabilities for the world's worst terrorist organization – the IRGC – by dealing with notorious fronts for the IRGC and pledging to assist with Iran's "security" agenda – all while fraudulently concealing it from all, including their shareholders. While doing so, MTN, ZTE, and Huawei also paid protection money directly to the IRGC's Afghan proxies, the Taliban.

15. MTN, ZTE, and Huawei are three of the worst corporate sponsors of terrorism in the history of the ATA. As a result, this case is likely to be different than a typical ATA case because of what Defendants have done, and this Complaint is longer than many ATA complaints. MTN, ZTE, and Huawei each funneled hundreds of millions in value to the terrorists in nearly every conceivable modality of terrorist fund transfer: direct transactions with FTO fronts while knowing (and not caring) about the FTO relationship; illicit acquisition of valuable American technologies; procurement bribes; "free goods" kickbacks; black market purchasing; cash flow from the companies; and so on.

16. The evidence regarding Defendants' intent is even worse. Like the IRGC fronts with whom they did business, MTN, ZTE, and Huawei made shocking admissions in writing, and then destroyed everything to try to cover their tracks (none succeeded completely). Some Defendants lied to federal law enforcement. Witness intimidation was common. Innocent Canadians were kidnapped to extort the United States and Canada.

17. MTN's, ZTE's, and Huawei's conduct, spending amount, and terrorist tradecraft is startlingly like how a State Sponsor of Terrorism acts—hundreds of millions of dollars in direct funding to terrorists, critical technical support that aids their victory given with the hope that it will occur, and a commitment to never-ending lies, falsehoods, and deceptions no matter how much evidence accumulates or how ridiculous it becomes.

18. MTN, ZTE, and Huawei may have learned this “never stop lying” tactic from their client, the IRGC, which is notorious amongst intelligence professionals for being one of the world's most persistent long-term liars, capable of sustaining a lie for decades.

19. MTN Group continues to openly conspire with multiple FTOs in plain sight. This is not normal, nor is it acceptable, but it is damning proof that MTN Group conspired with them all along.

20. MTN Group is currently the joint venture partner of known fronts for an FTO so committed to terror that it midwived, and controlled thereafter, a mine run of additional FTOs: Lebanese Hezbollah (FTO); Jaysh al-Mahdi Special Group Ka'taib Hezbollah (FTO); Jaysh al-Mahdi Special Group Asaib Ahl al-Haq (FTO); al-Qaeda-in-Iraq (FTO); Ansar-al-Islam (FTO). The list goes on.

21. MTN is unrepentant about its embrace of FTO terrorist fronts for cash, even though: (i) in 2012, a whistleblower heroically exposed MTN's secret deal, resulting in MTN's public humiliation in South Africa after the formerly iconic company became a subject of national mockery that year; (ii) also in 2012, a competitor, Turkcell, sued MTN for the latter having pilfered the former's lucrative contract out from under them; (iii) in 2019, being sued by hundreds of American victims of terrorist attacks in Afghanistan under the ATA concerning MTN's protection payments in Afghanistan; and (iv) being sued by Plaintiffs in the instant case.

22. Why would a publicly traded South African company like MTN Group do this? Money. MTN Irancell, the joint venture at issue, is MTN Group's cash cow and is, depending on metrics, either the second or third largest subscriber market in MTN Group's entire global portfolio. MTN Group concluded that it and its shareholders could reap billions of dollars in profits and lock in the single best international telecoms market opportunity in decades if it could achieve a meeting of the minds with the Iranian Shareholders who controlled Irancell.

23. To make billions of dollars running Iran's telecommunications with their IRGC partners, MTN, ZTE, and Huawei had to fully commit themselves worldwide to corporate criminality on a massive scale. These three companies combined to enable unprecedented aid to terrorists, which included, among other things:

- (i) a secret, direct, written, terrorist joint venture agreement signed by an active, senior-ranks Iranian terrorist, on the one hand, and the CEO of MTN, on the other;
- (ii) direct contractual obligations with Iranian entities known to be controlled by IRGC fronts, whereby banned technology useful to terrorists was transferred, and entire telecommunication systems used by the terrorists were assembled, used, and maintained;
- (iii) a nearly two decade-long Conspiracy that operationalized the secret deal into a technological, financial, services, and communications supply chain for the world's worst transnational terrorist organization;
- (iv) a large publicly traded company that refuses, even now, to exit its conspiracy with the IRGC, even after it has been publicly outed and even after the IRGC was designated as an FTO; and
- (v) shocking bribery, including tens of millions of "free goods" bribes designed to be diverted by terrorist to the black market, and large U.S. Dollar wire transfers after the bribe recipient performed his or her illicit deed.

24. To attack the citizens protected by the world's most powerful military in Iraq and Afghanistan and Iraq after 2003, Hezbollah, the Qods Force, and Regular IRGC organized a transnational terrorist alliance – a NATO for Islamists – that included both Shiite and Sunni organizations, and stretched throughout the Middle East, from Syria to Afghanistan.

25. In Iraq, not only did the IRGC helped stand up an alliance of Shiite terrorists that attacked Americans there, the IRGC also simultaneously sponsored al-Qaeda's terrorist proxies in Iraq, who shared the same goal as its Shiite proxies: kill Americans to drive the U.S. out.

26. The IRGC's ambitions did not stop at Iraq. As Hezbollah intensified its terror campaign in Iraq, the IRGC pursued a similar campaign against the Americans on Iran's other flank: Afghanistan. Like its role in Iraq, the IRGC provided comprehensive and critical support to the leaders of the anti-American alliance in Afghanistan and Pakistan, which operated as a terrorist "Syndicate" that was led by al-Qaeda and the Taliban.

27. In Afghanistan, the IRGC furthered the Conspiracy by funding, arming, training, logistically sustaining, and providing safe havens to al-Qaeda and the Taliban, who followed a similar Joint Cells approach as the IRGC, and for similar reasons. In the twenty years between 9/11 and the American withdrawal from Afghanistan, the IRGC, including its Hezbollah Division and Qods Force, prosecuted a grinding, global terrorist campaign, which it supported from a latticework of cells arrayed across six continents. The grim result: more than 4,000 Americans were killed in terrorist attacks in Afghanistan and Iraq by designated terrorist groups that were funded, armed, and logistically sustained by the IRGC. Indeed, each of the designated terrorist groups were members of the same global terrorist Conspiracy led by the IRGC.

28. Every Plaintiff is an American who was injured, or whose loved one was killed, between 2012 and 2014 in attacks that occurred in Syria and Afghanistan in furtherance of the IRGC Conspiracy. While three Plaintiffs' loved ones worked to stabilize Afghanistan, they were attacked by U.S. Government-designated terrorist organizations that participated in an IRGC-backed, Hezbollah-led terrorist Conspiracy campaign that MTN's, ZTE's, and Huawei's transactions helped finance, arm, support, conceal, and upgrade.

29. MTN, ZTE, and Huawei helped revolutionize the efficiency of the Big Data management practices and capabilities of Hezbollah and the Qods Force, in addition to the “regular” IRGC inside of Iran. It is impossible to overstate the scale of the carnage that followed Defendants’ decision to midwife the IRGC, including its Hezbollah Division and Qods Force, into the modern, networked, Big Data world.

30. Prior to Defendants, Hezbollah, the Qods Force, and Regular IRGC had the will but not the modern gear. While the IRGC had the scale of a multinational corporate behemoth – tens of thousands of personnel, consultants, agents, and partners, spanning dozens of countries on six continents – the IRGC lacked even rudimentary network computing technologies.

31. By 2004, the IRGC was surrounded on both flanks by “the Great Satan,” and the enormous technological gap between the IRGC and its mortal enemy – the “Big Data Gap” – forced the IRGC to do something drastic, which it had never done before: bring in foreign companies to revolutionize Iran’s computing and telecommunications infrastructure.

32. Two problems, however, still confronted Hezbollah, the Qods Force, and Regular IRGC. *First*, the IRGC knew that most large technology companies would have nothing at all to do with them. The IRGC also knew what any intelligence operative knows: that large telecom and networking computing companies come from a generally ethical industry that has never experienced a major terrorist finance scandal and are internationally notorious within the telecoms industry for being unabashed patriots. *Second*, and worse still, if the IRGC wanted to acquire the key technologies that it had determined were essential to prosecuting its terror campaign, it could not avoid an outcome in which the IRGC, indirectly, needed to reach into America’s markets, and acquire embargoed dual-use technologies on an industrial scale while

avoiding detection by the U.S. government and its responsible corporate allies, in a race where any stumble would likely expose (and hurt) the entire scheme.

33. The solution to both? Find some corporate criminals, bring them into the circle of trust, and count on their limitless greed. Enter Defendants. Since the 1979 revolution, the IRGC has always sought to kill Americans in large numbers. What it lacked was not the will, but the capabilities. After 9/11, the story remained the same – until MTN, ZTE, and Huawei answered the IRGC’s call for multinational corporate assistance to its “security” operations. What Hezbollah, the Qods Force, and Regular IRGC had never had – until Defendants – were true, established multinational corporate criminal partners. And Defendants furnished the IRGC three: MTN Group, ZTE Corporation, and Huawei Co. One has pleaded guilty (ZTE); one is currently defending itself in a criminal trial in this District (Huawei); and one is defending itself in South Africa (MTN).

34. After 9/11, the IRGC coordinated a grand alliance of Islamist terrorists to attack Americans in the Middle East. On the eve of the U.S. invasion of Iraq, the IRGC’s leadership and Hezbollah agreed to prepare, instigate, and sustain a nationwide campaign of terror against Americans in Iraq, which was planned and authorized by the IRGC’s lead foreign terror agent, Hezbollah. To sustain an ever-escalating terrorist campaign against the United States in Iraq, and later Afghanistan, Iran relied upon Hezbollah, which, in turn, depended upon IRGC funding and illicitly sourced gear from a constellation of IRGC, including Hezbollah and the Qods Force, terrorist fundraising and logistics cells scattered across dozens of countries on six continents.

35. To sustain their insurgency, the terrorists relied on two substantial funding streams: sources within Iran, and sources from the latticework of IRGC, Hezbollah and Qods Force logistics and fundraising cells across the globe. Cash flow from the telecom company

Irancell was either the largest or second largest source of cash flow from any IRGC front and caused hundreds of millions per year to flow to the IRGC, including \$4.2 billion between 2005, when MTN Group bribed its way to the lucrative Irancell license that was controlled by the IRGC (resulting in MTN Irancell), and 2013 – approximately \$500 million per year. Similarly, the global fundraising and logistics cells coordinated cash flows from narcotics smuggling, and the Qods Force’s and Hezbollah’s various transnational criminal rackets, e.g., collecting 10%-20% “taxes” as *khums* from allied businesspeople in Dubai, U.A.E., or Pretoria, South Africa.²

36. Given the transnational nature of the Conspiracy they led, the Qods Force and Hezbollah depended upon illicitly sourced, embargoed American communications and information technologies, which they acquired through Defendants MTN Group, MTN Dubai, ZTE Corp., ZTE TX, ZTE USA, Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom. Defendants’ conduct changed the trajectory of the terrorist campaign in Iraq and Afghanistan by revolutionizing the communications capabilities of both Hezbollah and the Qods Force and crippling the ability of U.S. forces in Iraq and Afghanistan to detain Qods Force and Hezbollah operatives in the region – because we could almost never find them. Because of Defendants’ choice to join the IRGC Conspiracy, Plaintiffs suffered the consequences.

37. MTN Group, ZTE Corp. and Huawei Co. entered the Conspiracy through secret deals to which their senior leaders agreed on their behalf, with IRGC operatives similarly agreeing on the IRGC’s behalf, necessarily including the IRGC’s external terrorist arms, the Qods Force and Hezbollah Divisions. This case is about that IRGC structure: from the terrorists’

² *Khums* are a form of fundraising in the Muslim faith analogous to tithing in the Christian faith, under which pious Muslims contribute between 10% to 20% of their income to a designated recipient. Hezbollah, the Qods Force, and Regular IRGC al-Qaeda, and the Taliban, including its Haqqani Network, have long solicited financial contributions styled as *khums*.

fundraising and logistics fronts (like the terrorist front disguised as a charitable trust, the Bonyad Mostazafan) to their strategies for illicitly sourcing U.S. Dollars and weapons technologies (like using agents, cut-outs, and intentional overpayments in Dubai), and raising money (through bribes, taxes, and front company cash flows), to their strategy for concealing the scheme (through removing U.N. sanctions that interfered with front companies necessary to the scheme), to their ability to securely communicate with one another (through illicitly obtained American phones), to their ability to better surveil kidnapping targets and anticipatory Quick Reaction Forces in response (from enhanced computing technologies) and finally, to their ability to build source the small arms, ammunition, and training necessary to successfully execute small arms attacks that punched through the cocoon of body armor that protected Americans (through a host of illicit technologies illegally sourced from the U.S.).

38. MTN Group, ZTE Corp., and Huawei Co. signed either literal terrorism joint venture agreements and/or entered into contracts with known IRGC fronts. MTN Group kept its agreement locked in a safe, concealed from the world. On information and belief, ZTE Corp. and Huawei Co., practicing better terrorist tradecraft than their sloppy co-conspirators at MTN Group, smartly destroyed their copies, but their parallel performance to MTN Group confirms their agreement all the same.

39. Ever since, publicly, MTN, ZTE and Huawei variously lied, dissembled, intimidated witnesses, destroyed evidence, all to avoid admitting the obvious: that they directly armed, funded, and enabled the communications of Hezbollah, the Qods Force, Regular IRGC, and the IRGC's proxies in Iraq, Iran, Lebanon, and Syria, as well as Qods Force and Hezbollah support cells from around the world, stretching from Syria to Afghanistan.

40. MTN Group, ZTE Corp., and Huawei Co. are each culpable. Each did, essentially, the same thing. The only difference is that MTN Group's secret vault of smoking documents were leaked by a whistleblower in March 2012, revealing the scheme MTN Group had fraudulently concealed from the world, its own shareholders, the South African government, the U.S. government, and the U.A.E. government, to name but a few.

41. The MTN Group document revelation in 2012 did not just reveal MTN Group's scheme. Critically, it outed the *IRGC's terrorist tradecraft* when it comes to virtually every facet of the terrorist logistics, funding, and communications chains. MTN Group's conduct is not just probative of what MTN Group itself did; as informed by information that emerged years later, it shows what the IRGC demanded of *every* corporate business partner in this space.

Consequently, MTN Group's conduct offers a reasonable inference regarding the conduct of ZTE Corp. and Huawei Co., as well as that of their mutual business partner – the IRGC.

42. Like MTN Group, ZTE Corp. and Huawei Co. also joined the Conspiracy and also fraudulently concealed their participation by following the same Hezbollah/Qods Force playbook that MTN Group followed. Unlike MTN, however, ZTE and Huawei did not experience their own whistleblower revolts until later, but eventually, everyone got caught. MTN Group has been enmeshed in litigation for nearly a decade. And ZTE and Huawei were both investigated by U.S. law enforcement and charged with serious crimes. From these cases, there is overwhelming evidence that Hezbollah, the Qods Force, and Regular IRGC relied upon ZTE and Huawei, just as these IRGC constituents did with respect to MTN, to surreptitiously acquire U.S. Dollars and vital U.S. technologies critical to every aspect of the terrorist enterprise.

43. MTN Group, ZTE Corp., and Huawei Co. were one in spirit with the terrorists. Each pledged, in writing, their commitment to aiding the IRGC's "security" – which all involved

understood to be a euphemism for anti-American terror. They did this because IRGC domination of the Middle East was great for their profits and, with respect to ZTE Corp. and Huawei Co., the victory of the IRGC over the U.S. served the hostile national security objectives of the Chinese Communist Party, which sought to aid Shiite terrorists in the region to inflict pain on Americans in the Middle East and cause the United States to withdraw.

44. After entering the Conspiracy with known IRGC fronts called Irancell and TCI, MTN Group, ZTE Corp., Huawei Co., and their respective subsidiaries, knowingly partnered with notorious fronts for Hezbollah, such as the Bonyad Mostazafan. Through such business, MTN, ZTE, and Huawei provided direct financial support, revenue, U.S.-origin, embargoed technology and equipment, and training and expertise—all of which the Hezbollah and the Qods Force provided to the IRGC’s terrorist allies operating in Afghanistan and Iraq (and consequently, Syria)—and all of which was used to target to kill and injure Americans, including Plaintiffs.

45. As long-term strategic partners who worked closely together in Iran, MTN, ZTE and Huawei all understood their counterparties were notorious terrorist fronts used to raise money and source weapons for the Qods Force, Hezbollah, and their proxies and/or allies in places like Afghanistan, Syria, and Iraq. Defendants knew or were willfully blind to the fact that their “business” with terrorist fronts was serving the terrorists’ ends but did it anyway.

46. Hezbollah, the Qods Force, and Regular IRGC used the IRGC’s relationships with MTN Group, ZTE Corp., and Huawei Co. to optimize Iran’s terrorist enterprise by bolstering the financial and technical capacities of Iran’s terrorist proxies.

47. Through the IRGC’s, including Hezbollah’s and the Qods Force’s, transactions with MTN Group, ZTE Corp., and Huawei Co., Hezbollah, the Qods Force, and the IRGC’s

terrorist proxies were able to evade the international sanctions regime to source weapons and weapons components for terror, modernize their communications systems to better encrypt signals traffic, improve their surveillance and intelligence capabilities, and generate tens of millions in annual revenue to fund attacks – all of which Hezbollah, the Qods Force, and the IRGC’s proxies in Afghanistan, including al-Qaeda and the Taliban, used to attack Americans in Afghanistan from 2012 through 2017.

48. The total value of the money, technology, and services that Hezbollah, the Qods Force, and Regular IRGC obtained via MTN Group’s, ZTE Corp.’s, and Huawei Co.’s business with the IRGC collectively extracted likely ranges into the hundreds of millions of U.S. Dollars in cash and cash equivalents—and the terrorists used those resources to pay for terrorist proxy attacks in Afghanistan and Syria.

49. But this case is not just about money; the technology that MTN Group, ZTE Corp., and Huawei Co. provided to the IRGC, which inevitably flowed through to IRGC proxies al-Qaeda (including AQI and ANF) and the Taliban, was uniquely important to the terrorists, enabling them to inflict maximum damage because, among other things, it allowed them to spy on Americans, avoid detection, clandestinely communicate, build and detonate more effective bombs, and develop more accurate and lethal rockets. And on top of the money and the technology, Defendants also provided substantial ongoing logistical and operational aid for the IRGC’s, including its Hezbollah Division’s and Qods Force’s, terrorist enterprise.

50. This is not a case about one or two alleged rogue employees who engaged in a frolic and detour that resulted in a company’s money reaching terrorists. Here, each Defendant’s executives were thoroughly implicated in the terrorist finance and logistics scheme, and actively supported doing business with known terrorist fronts.

51. MTN's leadership, for example, mocked those who raised concerns about the risks of becoming joint venture partners with two notorious Iranian terror fronts: When queried by investors about the "risk of doing business with Iran," MTN's then-CEO "laughed off" such questions, joking that "[MTN] hadn't budgeted for bomb shelters or anything like that."

52. ZTE's executives were similarly culpable. According to the then-Acting Assistant Attorney General, Mary B. McCord, "ZTE engaged in an elaborate scheme to acquire U.S.-origin items, send the items to Iran and mask its involvement in those exports," and the plea agreement ZTE signed on behalf of itself and its subsidiaries "alleges that the highest levels of management within the company approved the scheme."

53. Huawei was much the same. Acting U.S. Attorney for the Eastern District of New York Nicole Boeckmann announced a deferred prosecution agreement by Huawei Co's CFO wherein she "[took] responsibility for her principal role in perpetrating a scheme to defraud a global financial institution," and admitted in the related statements of facts that she had "while acting as the Chief Financial Officer for Huawei, . . . made multiple material misrepresentations to a senior executive of a financial institution regarding Huawei's business operations in Iran" and that she and "her fellow Huawei employees engaged in a *concerted effort to deceive global financial institutions, the U.S. government and the public about Huawei's activities in Iran.*"

54. In August 2021, America withdrew from Afghanistan. A well-organized, cohesive, and integrated Taliban seized the country. Tens of thousands of Afghan heroes fled everyone and everything they knew, for a new life in the U.S.

55. Defendants' business partners and their "Iranian Shareholders" celebrated the terrorists' victory (undoubtedly joined, as discovery is likely to reveal, by many of MTN's, ZTE's, and Huawei's non-U.S. employees and management).

56. MTN's, ZTE's, and Huawei's transactions, and the terrorist attacks they funded, were acts of "international terrorism." 18 U.S.C. § 2333(a).

57. The al-Qaeda/Taliban attacks against Plaintiffs in Afghanistan were "planned," "authorized," and jointly "committed" by al-Qaeda, 18 U.S.C. § 2333(d)(2). The kidnapping attack against Plaintiff Matthew Schrier was "committed" by al-Nusra Front and was "planned" and "authorized" by al-Qaeda and al-Qaeda-in-Iraq.

58. Plaintiffs are U.S. citizens, and their family members, who were killed or wounded in terrorist attacks committed by the IRGC's terrorist proxies in Afghanistan and Syria, with material support from the IRGC. As alleged below, Plaintiffs are entitled to recover for their injuries under the federal Anti-Terrorism Act. MTN, ZTE, and Huawei are liable under the ATA, 18 U.S.C. § 2333(d)(2), because they aided and abetted the campaign by Hezbollah, the Qods Force, al-Qaeda (including its branches in Iraq and Syria), and the Taliban, to commit terrorist attacks in Afghanistan and Syria that were committed, planned, or authorized by al-Qaeda.

59. Each Plaintiff was killed or injured by a terrorist attack committed by terrorists who received direct funding, weapons, weapons components, communications technology, and/or operational support made possible by MTN's, ZTE's, and Huawei's conduct.

DEFENDANTS

A. The MTN Defendants

60. Defendant MTN Group Limited ("MTN Group," together with its subsidiaries, "MTN") is a South African telecommunications company whose stock trades publicly on the Johannesburg Stock Exchange under the ticker symbol MTN:SJ. Its principal place of business is in Roodepoort, South Africa.

61. Defendant MTN Irancell is a joint venture between MTN Group, which has a 49% stake and is not in charge, and the Bonyad Mostazafan and Iran Electronics Industries (“IEI”), which collectively own a 51% stake and are fronts for the IRGC, including its Hezbollah Division and Qods Force (sometimes abbreviated “IRGC-QF”). MTN Irancell is an Iranian company, and its principal place of business is in Tehran, Iran. MTN Irancell operates as, and MTN Irancell’s employees and agents work as operatives for, a front for the IRGC, including its Hezbollah Division and Qods Force.

62. Defendant MTN (Dubai) Limited (“MTN Dubai”) is a wholly owned subsidiary of MTN Group. It is a Dubai company, and its principal place of business is in Dubai.

B. The ZTE Defendants

63. On information and belief, Defendant ZTE Corporation (“ZTE Corp.,” together with its subsidiaries, “ZTE”), is a Chinese corporation with a principal place of business in Guangdong Province, People’s Republic of China.

64. Defendant ZTE (USA), Inc. (“ZTE USA”) is a New Jersey corporation that is a wholly-owned subsidiary of ZTE Corp., headquartered in Richardson, Texas. On March 7, 2017, ZTE and its subsidiaries (including, on information and belief, ZTE USA) entered into a settlement agreement with the U.S. Department of the Treasury’s Office of Foreign Assets Control (the “ZTE 2017 OFAC Settlement”). Therein, ZTE USA admitted, *inter alia*, (a) it knowingly participated in a scheme with ZTE Corp. to illegally transfer over \$39 million in U.S. goods to Iran, and otherwise (b) conducts business for ZTE Corp. on its behalf. For these reasons, allegations regarding “ZTE” in this Complaint apply equally to ZTE USA, because ZTE USA was instrumental in the scheme alleged herein by ZTE generally.

65. Defendant ZTE (TX) Inc. (“ZTE TX”) is a wholly-owned subsidiary of ZTE Corp. ZTE TX is a corporation organized and existing under the laws of the State of Texas with

its principal place of business in Milpitas, California. As a subsidiary of ZTE, ZTE TX also was party to the ZTE 2017 OFAC Settlement. In the ZTE 2017 OFAC Settlement, ZTE TX admitted, *inter alia*, that it (a) knowingly participated in a scheme with ZTE Corp. to illegally transfer over \$39 million in U.S. goods to Iran and otherwise (b) conducts business for ZTE Corp. on its behalf. For these reasons, allegations of acts after ZTE TX's formation regarding "ZTE" in this Complaint apply equally to ZTE TX, because ZTE TX was instrumental in the scheme alleged herein by ZTE generally.

C. The Huawei Defendants

66. On information and belief, Defendant Huawei Technologies Co., Ltd. ("Huawei Co.," together with its subsidiaries and affiliates, "Huawei") is a Chinese company with a principal place of business in Shenzhen, Guangdong Province, People's Republic of China. Huawei Co. is owned by its parent company Huawei Investment & Holding Co., Ltd. ("Huawei Holdings"), a Chinese company registered in Shenzhen, Guangdong, People's Republic of China.

67. Defendant Huawei Technologies USA Inc. ("Huawei USA") is a corporation organized under the laws of the State of Texas with its principal place of business in Addison, Texas. Huawei USA is a wholly-owned indirect subsidiary of Huawei Co. On February 28, 2023, Huawei USA notified known claimants that in accordance with Section 11.052(a)(2) of the Texas Business Organizations Code, it had passed a dissolution resolution effective as of January 16, 2023, and has commenced a winding-up process upon the conclusion of which Huawei USA intends to terminate its legal existence under Texas law.

68. Defendant Huawei Device USA Inc. ("Huawei Device USA") is a Texas corporation that is organized under the laws of the State of Texas with its principal place of business in Addison, Texas. Huawei Device USA is a subsidiary of Huawei Co. and Huawei Co.'s parent, Huawei Holdings. On February 28, 2023, Huawei Device USA notified known

claimants that in accordance with Section 11.052(a)(2) of the Texas Business Organizations Code, it had passed a dissolution resolution effective as of January 16, 2023, and has commenced a winding-up process upon the conclusion of which Huawei Device USA intends to terminate its legal existence under Texas law.

69. Defendant Futurewei Technologies, Inc. (“Futurewei”) is a corporation organized under the laws of the State of Texas with its principal place of business in Santa Clara, California. Futurewei is a subsidiary of Huawei Co. and Huawei Co.’s parent, Huawei Holdings.

70. Defendant Skycom Tech Co., Ltd. (“Skycom”) is a corporation registered in Hong Kong with its principal place of business located in Tehran, Iran. As of 2007, Skycom was wholly-owned by Huawei Co.’s subsidiary Hua Ying (“Hua Ying”). In November 2007, Huawei Co. directed Hua Ying to transfer its shares in Skycom to Calicula Holdings Ltd. (“Calicula”), another a subsidiary controlled by Huawei Co.

JURISDICTION AND VENUE

71. This Court has subject-matter jurisdiction under 18 U.S.C. § 2338 and 28 U.S.C. § 2331, and has personal jurisdiction over each of the Defendants under Federal Rule of Civil Procedure 4(k)(1) and/or 4(k)(2), and 18 U.S.C. § 2334(a).

72. MTN’s acts in the United States, including but not limited to obtaining U.S.-origin technology and equipment for export to Iran, and targeting the United States, including by entering into transactions with fronts, operatives, and agents for the IRGC, including its Hezbollah Division and Qods Force, that were intent on harming United States nationals in Iraq, make appropriate this Court’s jurisdiction over MTN.

73. MTN does business in New York, including by procuring U.S.-origin goods and services from companies located in the U.S., including New York, for the IRGC’s, including its Hezbollah Division’s and Qods Force’s, fronts, agents, and operatives, maintaining accounts

with financial institutions located in New York, including, on information and belief, a loan facility with Citibank and a depository account with the Bank of New York, using the New York-based financial system and institutions to manage cash flow for MTN Group, MTN Irancell, and MTN Dubai, utilizing a bank account in New York to wire funds to an agent of the IRGC, including its Hezbollah Division and Qods Force, to consummate a bribe relating to MTN's acquisition of the Irancell license, and working with a New York-based financial institution to issue a sponsored American depository receipt (ADR).

74. ZTE's acts in the United States, including but not limited to (i) obtaining U.S.-origin technology and equipment for export to Iran, including but not limited to working with and through, ZTE USA and ZTE TX to do so, and (ii) targeting the United States, including by entering into transactions with fronts, operatives, and agents for the Hezbollah, the Qods Force, and Regular IRGC that were intent on harming United States nationals in Afghanistan, make appropriate this Court's jurisdiction over ZTE Corp., ZTE USA, and ZTE TX.

75. ZTE does business in New York, including by selling cell phones and telecommunications equipment. ZTE USA is registered to do business in the state of New York, and its Registered Agent is Incorp Services Inc. of Albany, NY. ZTE also maintains accounts with financial institutions, located in New York, which, on information and belief, ZTE utilized in furtherance of their scheme alleged herein. Additionally, the U.S. Attorney's Office for the Southern District of New York is investigating ZTE for bribery, and on information and belief the conduct being investigated occurred in New York. ZTE has consistently, during the relevant period, entered into major partnership and business deals in New York, and typically announces new product offerings at events physically in New York. Senior ZTE USA officials have declared that New York is a community "in which we live and work." Further, ZTE entered into

key partnership with counterparties in New York necessary for ZTE to obtain the devices and technology that its IRGC-front counterparties sought (and which ZTE delivered), including (i) an agreement with a counterparty in New York to source rugged glass fronts for their cell phones, which was necessary for the rough physical environments in which the terrorists operate, and (ii) an agreement with a counterparty in New York that assisted ZTE with enhancing the security features on its smartphones, which was necessary for the terrorists to be able to avoid detection and operate without surveillance.

76. Huawei's acts in the United States, including but not limited to, obtaining U.S.-origin services, technology, and equipment for export to Iran, working with and through Skycom, Futurewei, Huawei Device USA, and Huawei USA to do so, and targeting the United States, including by entering into transactions with fronts, operatives, and agents for Hezbollah, the Qods Force, and Regular IRGC that were intent on harming United States nationals in Afghanistan, make appropriate this Court's jurisdiction over Huawei Co., Huawei USA, Futurewei, Huawei Device USA, and Skycom.

77. Huawei does business in New York, including by selling cell phones and telecommunications equipment. Huawei also maintains accounts with financial institutions, located in New York, which, on information and belief, Huawei utilized in furtherance of their scheme alleged herein. Additionally, the U.S. Attorney's Office for the Eastern District of New York is currently pursuing criminal charges against Huawei, including its American subsidiaries Futurewei and Huawei Device USA, for, *inter alia*, their unlawful conduct, relating to their Iranian business interests, including conduct in the Eastern District of New York.

78. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to the claims occurred in this District.

FACTUAL ALLEGATIONS

I. SINCE THE ISLAMIC REVOLUTION IN 1979, THE ISLAMIC REVOLUTIONARY GUARD CORPS, OR IRGC, HAS FOMENTED AND SUSTAINED ANTI-AMERICAN TERRORISM

79. The 1979 Iranian Revolution was fueled in large part by militant anti-Americanism. Eliminating the United States’ role in the region surrounding Iran – including through violence – was and remains a central tenet of Iranian foreign policy. Since the Iranian Revolution, Iran has engaged in and supported acts of terrorism directed at the United States and its allies as an instrument of Iran’s foreign policy. *See, e.g., Cabrera, et al. v. Islamic Republic of Iran*, 2022 WL 2817730, at *9 (D.D.C. July 19, 2022) (“*Cabrera*”).

80. Iran’s support of terrorist proxies like Hezbollah, Hamas, al-Qaeda, and the Taliban is well-documented. As a result of Iran’s longstanding support of anti-American terrorism, the U.S. State Department formally designated Iran as a State Sponsor of Terrorism in 1984, and has maintained that designation at all times since. In 2007, it described Iran as “the most active state sponsor of terrorism” in the world and “a threat to regional stability and U.S. interests in the Middle East because of its continued support for violent groups.”

81. Iran is hostile to the United States and its allies. Enmity toward America is foundational for the Iranian regime in general, and most of all, for Grand Ayatollah Khamenei, who is the effective leader of the Islamic Revolutionary Guard Corps, including its Hezbollah Division and Qods Force, both of which report to him personally as head of the IRGC.³

³ The IRGC is comprised of the Hezbollah Division, more popularly known as Lebanese Hezbollah or Hezbollah, the Qods Force, and the Regular IRGC. In this complaint, every reference to “IRGC” also includes Hezbollah, the Qods Force, and the Regular IRGC

A. Islamic Revolutionary Guard Corps

82. Iran carries out its support of terrorism largely through the IRGC.⁴ *See, e.g., Cabrera* at *9. As the U.S. Treasury Department noted in 2010 when it designated certain IRGC officials pursuant to Executive Order 13224, “Iran also uses the . . . IRGC . . . to implement its foreign policy goals, including, but not limited to, seemingly legitimate activities that provide cover for intelligence operations and support to terrorist and insurgent groups.”

83. The IRGC was established to safeguard the revolution, meaning, to pursue violence inside of Iran, i.e., terrorism against its own people, and external to Iran, i.e., terrorism against America and Israel, whom the IRGC considered to be the “Great Satan” and “Little Satan,” respectively. *See, e.g., Cabrera* at *9. Articles 150 and 154 of Iran’s Constitution order the IRGC to export Iran’s Revolution by aiding insurgents: the IRGC is responsible for “guarding the revolution and its achievements,” meaning, exporting the Islamic Revolution (Art. 150),⁵ and Iran “supports the just struggles of the *mustad’afun* [downtrodden] against the *mustakbirun* [oppressors] in every corner of the globe” (Art. 154). Thus, Iran’s constitution directly embraces proxy terror (“the just struggles of the downtrodden”) targeting the U.S. (i.e., “against the oppressors”).⁶

⁴ In 1990, the IRGC transferred activities outside Iran to its subordinate branch, the Qods Force.

⁵ Under Iran’s revolutionary doctrine, the Iranian government posits that it must always remain on the attack with respect to its promotion of insurgents against the Great Satan because, if Iran were to fall back (according to this paranoid theory), the U.S. would overrun Iran. Consequently, inside Iran and around the world, people familiar with Iran and the IRGC understand that references to “guarding the revolution” are **not** defensive, but rather, are **offensive** because, under the paranoid Iranian view, the only way to “guard the revolution” is to go on the attack outside of Iran, through proxy terror campaigns. Any suggestion to the contrary is, quite literally, IRGC terrorist propaganda.

⁶ When the Iranian government references “the oppressors” without any specification as to whom, that **exclusively** means only two countries: the United States and Israel. This is so

84. In an analysis of MTN Irancell published by NATO, Monika Gill explained that under the IRGC’s official, publicly communicated security doctrine, the IRGC’s “security” interests are defined as “leading an ongoing resistance” in a zero-sum fight against the United States.⁷ Indeed, on November 22, 2014, MTN Irancell’s CEO publicly aligned MTN Irancell with the IRGC’s “resistance” narrative and admitted that MTN Irancell serves the IRGC’s terrorist “resistance” efforts as part of MTN Irancell’s corporate “social responsibility” and stated, among other things, that MTN Irancell’s “development” of communications technology “will make some of the objectives pursued by the resistive economy come true,” including “[r]esistance against the threatening elements.”⁸

85. Between 1984 and 2007, the U.S. government repeatedly designated the Iranian government for the IRGC’s support of anti-American terror, and implemented terrorism sanctions-related regulations which broadly prohibited economic transactions with any entities controlled by the Iranian government.⁹ (Such prohibitions generally endured at all relevant times.)

because the Iranian regime was founded in direct opposition to us and our ally, and Iran’s founding documents mention no other hostile actor beyond the U.S. and Israel. Any suggestion to the contrary is, literally, Iranian propaganda designed for a Western audience.

⁷ Monika Gill, *Capitalism, Communications, and the Corps: Iran’s Revolutionary Guard and the Communications Economy*, Defence Strategic Communications: The Official Journal of the NATO Strategic Communications Centre of Excellence, at 97 (Autumn 2020) (“Gill”).

⁸ ICTNA (Iran), *Irancell Brings 4G to Iran* (Nov. 22, 2014), <https://www.ictna.ir/id/065513/>.

⁹ On January 19, 1984, Iran was designated as a State Sponsor of Terrorism pursuant to section 6 of the Export Administration Act of 1979 (50 U.S.C. § 4605), section 620A of the Foreign Assistance Act of 1961 (22 U.S.C. § 2371), and section 40 of the Arms Export Control Act (22 U.S.C. § 2780). The United States has maintained that designation at all times since. See also, e.g., Exec. Order 12957, 60 Fed. Reg. 14615 (Mar. 17, 1995). On August 21, 1997, President Clinton issued Executive Order 13059 to comprehensively prohibit trade intended to benefit, among other things, the IRGC, including its Hezbollah Division and Qods Force. Exec. Order 13059, 62 Fed. Reg. 44531 (Aug. 21, 1997). U.S. government regulations broadly prohibiting trade with Iran included, but were not limited to, 31 C.F.R. § 560.304 (defining “Government of

86. In April 2008, the U.S. State Department described Iran as “the most active state sponsor of terrorism” in the world and “a threat to regional stability and U.S. interests in the Middle East because of its continued support for violent groups.”

87. On May 27, 2009, the U.S. Treasury Department announced additional IRGC-related sanctions further reflecting the long-standing U.S. conclusion that the IRGC used its revenue to pay for Hezbollah’s operations and training activities and “provides hundreds of millions of dollars per year to Hizballah.”¹⁰

88. The IRGC has a long and well-documented history of assassinations, kidnappings, bombings, and arms dealing. It also regularly trains foreign terrorist proxies whose attacks promote Iran’s political goals, often working side-by-side with Hezbollah.

89. The IRGC has used Hezbollah and its proxies to commit terrorist attacks. While it is a Lebanese-based terrorist group, Hezbollah has pledged fealty to Iran’s Supreme Leader. As Ali Akbar Mohtashemi (a Hezbollah founder, former Iranian ambassador to Syria and Lebanon, and former Iranian Minister of Interior) explained, “[Hezbollah] is part of the Iranian rulership; [Hezbollah] is a central component of the Iranian military and security establishment; the ties between Iran and [Hezbollah] are far greater than those between a revolutionary regime with a revolutionary party or organization outside its borders.”

90. On April 15, 2019, the U.S. State Department designated the entirety of the IRGC, including the Regular IRGC and the Qods Force, as a Foreign Terrorist Organization, which completed the designation of every IRGC-related entity as an FTO.¹¹ Announcing the

Iran”), 31 C.F.R. § 560.313 (defining “entity owned or controlled by the Government of Iran”); and 31 C.F.R. § 560.314 (defining “United States person”).

¹⁰ U.S. Treasury Dep’t, *Treasury Targets Hizballah Network in Africa* (May 27, 2009).

¹¹ In 1997, the State Department designated Hezbollah – known to the IRGC as its own Hezbollah Division – as an FTO.

designation, President Trump explained that “the IRGC *actively participates in, finances, and promotes terrorism as a tool of statecraft*.”¹² According to the U.S. State Department’s public statement explaining the designation, Hezbollah, the Qods Force, and Regular IRGC have “been directly involved in terrorist plotting; its support for terrorism is *foundational and institutional*, and it has killed U.S. citizens.”¹³

91. When the State Department designated the IRGC as a Foreign Terrorist Organization, Secretary of State Michael R. Pompeo stated, among other things:

- (i) “This is the first time that the United States has designated a part of another government as an FTO. ... *[T]he Iranian regime’s use of terrorism as a tool of statecraft makes it fundamentally different from any other government.* ... “
- (ii) “For 40 years, the [IRGC] has actively engaged in terrorism and created, supported, and directed other terrorist groups.”
- (iii) “The IRGC institutionalized terrorism shortly after its inception, directing horrific attacks against the Marine barracks in Beirut in 1983 and the U.S. embassy annex in 1984 alongside *the terror group it midwifed, Lebanese Hizballah.*”
- (iv) “[The] Iranian regime not only supports terrorist groups, but engages in terrorism itself. This designation also brings unprecedented pressure on figures who lead the regime’s terror campaign, individuals like Qasem Soleimani. ... He *doles out the regime’s profits to terrorist groups across the region and around the world.*”¹⁴

92. As the world’s worst sponsor of terrorism, Iran was unique. It was not a “normal” government, but a regime that facilitated a climate where Hezbollah, the Qods Force, and the Regular IRGC relied upon the IRGC’s corporate allies to directly enable violence. As Ambassador Mark D. Wallace, of United Against Nuclear Iran (“UANI”), explained,

¹² Statement from the President on the Designation of the Islamic Revolutionary Guard Corps as a Foreign Terrorist Organization (Apr. 8, 2019) (emphasis added).

¹³ U.S. Dep’t of State, *Fact Sheet: Designation of the Islamic Revolutionary Guard Corps* (Apr. 8, 2019) (emphasis added).

¹⁴ Secretary of State Michael R. Pompeo, U.S. Dep’t of State, *Remarks to the Press* (Apr. 8, 2019) (emphasis added).

“[i]nternational organizations must also realize that their relationship with Iran is not just ... ‘business as usual,’ ... Put bluntly, Iran ... *should not be treated like a member in good standing* of international bodies.”¹⁵

B. Hezbollah

93. Hezbollah was and is the IRGC’s, including the Qods Force’s, lead terrorist proxy in the broader Middle East, serving, in effect, as the IRGC’s external terrorist operations arm in conjunction with Hezbollah’s close ally and patron, the Qods Force.

94. Hezbollah, translated as “Party of God,” “first emerged as a militia in opposition to the 1982 Israeli invasion of Lebanon”¹⁶ when the IRGC created Hezbollah as a subordinate part of the IRGC known as the “Hezbollah Division.”¹⁷

95. Hezbollah likewise views itself a part of the IRGC. In 1985, “Hezbollah publicly acknowledged its reliance on Iran, stating that “We abide by the orders of one single wise and just leadership, represented by ‘*Wali Faqih*’ [rule of the jurisprudent] and personified by Khomeini.” Hezbollah operatives swear a personal oath of loyalty to Iran’s Supreme Leader, Ayatollah Khamenei, and personally pledge to carry out their terrorist missions in his name.

¹⁵ Statement of the Honorable Mark D. Wallace, CEO United Against Nuclear Iran before the U.S. House of Representatives Committee on Foreign Affairs, *Iran Sanctions*, Congressional Testimony via FDCH (May 17, 2012) (emphasis added), 2012 WLNR 10405070 (“Wallace May 17, 2012 Testimony”).

¹⁶ Marc Lindemann (Captain, New York National Guard), *Laboratory of Asymmetry: The 2006 Lebanon War and the Evolution of Iranian Ground Tactics*, Military Review (May 1, 2010), 2010 WLNR 28507137 (“Lindemann, *Laboratory of Asymmetry*”). ““Although Iran was engaged in the Iran-Iraq War at the time of the Israeli occupation, Iran’s Islamic Revolutionary Guard Corps (IRGC) took the lead in organizing, training, and equipping Hezbollah ... Training at the IRGC camps became a prerequisite for membership in Hezbollah.” *Id.*

¹⁷ Michael Knights, *The Evolution of Iran’s Special Groups in Iraq*, Combating Terrorism Center at West Point, CTC Sentinel, Vol. 3, No. 11 (Nov. 2010) (“Knights, *The Evolution of Iran’s Special Groups in Iraq*”).

96. The IRGC directly funds its Hezbollah Division in the same manner as its Qods Force, as they are two sides of the same IRGC external terror coin. As the Defense Intelligence Agency (“DIA”) concluded with “high confidence” in 2010, “[e]lements of Iran’s Islamic Revolutionary Guard Corps ... provided direct support to terrorist groups, assisting in the planning of terrorist acts or enhancing terrorist group capabilities.”

97. On January 25, 1995, the United States designated Hezbollah as a Specially Designated Terrorist. On October 8, 1997, the United States designated Hezbollah as an FTO, and it has retained that designation ever since.

98. Hezbollah’s activities have stretched far beyond Lebanon’s borders. Hezbollah’s primary stated goal is the destruction of the United States and Israel, which it calls the “Great Satan” and the “Little Satan,” respectively.¹⁸ Hezbollah also frequently functions as a terrorist proxy for the IRGC, committing and orchestrating terrorist attacks abroad with the IRGC’s, including the Qods Force’s, support.

99. Hezbollah has coordinated terrorist attacks around the world primarily by acting through terrorist proxies. As Dr. Matthew Levitt has explained, “Hezbollah is extremely adept at recruiting members from local populations in areas where they have networks on the ground.”¹⁹ Hezbollah has trained and equipped these local proxies to carry out terrorist attacks on its behalf.

100. Hezbollah is and has always been widely understood to be Iran’s purpose-built anti-American and anti-Israeli Arab Shiite terrorist division, which the IRGC designed to integrate within the IRGC’s terror architecture, including, but not limited to, its financial,

¹⁸ See Times of Israel, *Nasrallah Proud that PM, Obama Discussed Hezbollah* (Nov. 11, 2015); Ariel Ben Solomon, *Nasrallah ‘Proud’ that Netanyahu and Obama Discussed Hezbollah in White House Meeting*, Jerusalem Post (Nov. 11, 2015).

¹⁹ Matthew Levitt, *Hezbollah: A Case Study of Global Reach*, Remarks to a Conference on “Post-Modern Terrorism: Trends, Scenarios, and Future Threats” at 4 (Sept. 8, 2003).

operational, and logistics networks, to ensure that Hezbollah was inseparable from the Regular IRGC and Qods Force and always remained a formal part of the IRGC. The IRGC built Hezbollah this way because the IRGC wanted to be able to control Hezbollah while maintaining the fiction that Hezbollah were merely “resistance” fighters. The IRGC’s ploy was key to facilitating its worst terrorist plots because the IRGC’s primary purpose when it created its Hezbollah Division was to secure the IRGC’s plausible deniability by interposing a buffer – Hezbollah – between the IRGC and the Americans whom the IRGC wanted to murder.

101. The IRGC has long relied on Hezbollah to aid the Qods Force’s efforts to supply al-Qaeda and its Taliban allies²⁰ as they targeted Americans in Afghanistan and Iraq:

- (i) The IRGC has relied upon Hezbollah and the Qods Force to aid attacks against Americans by al-Qaeda and its allies since the early 1990s (in the case of al-Qaeda and Ansar al-Islam) and/or shortly after 9/11 (in the case of the Taliban).
- (ii) Before 9/11, the IRGC, al-Qaeda, the Taliban, and their respective affiliates worked together to broker combined Islamist terrorist training activities at Taliban sites in Afghanistan, at which terrorists from Hezbollah, the Qods Force, al-Qaeda, the Taliban, Hamas, and Palestinian Islamic Jihad trained together to develop the long-term skills and relationships that bin Laden demanded under his corporate “always be closing” model of terror, which emphasized cross-pollination with every possible Islamist terrorist group as long as such group wanted to help al-Qaeda and its allies kill Americans.²¹

²⁰ The IRGC was essential to enabling transnational Sunni Islamist cooperation between Afghanistan/Pakistan and Iraq and maximizing the ability of al-Qaeda and Taliban terrorists in Afghanistan to leverage the personnel, funding streams, resources, and trainers available in Iraq in order to enhance the lethality of al-Qaeda and Taliban attacks in Afghanistan (and vice versa). For example, al-Qaeda relied upon the funding and logistical support provided by the IRGC to source CAN fertilizer from Pakistan (to use for bombs in Afghanistan and Iraq), secure cell phones from America (to be used for communications or as a cash equivalent “free good” valued at \$2,000 per phone), and narcotics trafficking and laundering assistance, which funded al-Qaeda’s and the Taliban’s attacks against Americans in Afghanistan, including those that injured Plaintiffs and their loved ones.

²¹ See, e.g., Hal Bernton, Mike Carter, David Heath and James Neff, *Going To Camp*, Seattle Times (Aug. 4, 2002) (“By [1998], al-Qaida training was formalized. There was even a textbook, available in Arabic, French and other languages. ... Trainees practiced with small arms, assault rifles and grenade launchers provided by the Taliban They learned about explosives and land mines. Representatives of terrorist groups, including Hamas, Hezbollah and Islamic Jihad, gave lectures on their organizations.”), 2002 WLNR 2584645.

- (iii) After 9/11, al-Qaeda, the IRGC, and their respective affiliates intensified their transnational terrorist alliance; the IRGC acted primarily through its Hezbollah and Qods Force operatives distributed in cells worldwide, while al-Qaeda and the Taliban, for their part, acted primarily through al-Qaeda- and Haqqani Network-related “polyterrorists” who served more than one member organization of the Syndicate, e.g., Sirajuddin Haqqani was a member of al-Qaeda and the Taliban.

C. Qods Force

102. As the U.S. State Department observed in 2016, “Iran used the [Qods Force] to implement foreign policy goals, provide cover for intelligence operations, and create instability in the Middle East. The Qods Force is Iran’s primary mechanism for cultivating and supporting terrorists abroad.” The Qods Force is the driving force behind Iran’s activities in Afghanistan, as well as in Iraq, Syria, and elsewhere in the Middle East.

103. The Qods Force is responsible to and directed by the Supreme Leader of Iran. Major General Qassem Soleimani was the chief of the Qods Force for more than twenty years and oversaw the Qods Force’s support for Hezbollah and its proxies to promote Iran’s policies throughout the region. Soleimani took his directions from Khamenei, with whom he shared a close personal relationship. Soleimani was killed in a U.S. airstrike in Baghdad, Iraq on January 3, 2020. Khamenei then appointed General Esmail Ghaani to replace Soleimani.

104. The Qods Force provides weapons, funding, and training for terrorist operations targeting American citizens, including for Hezbollah and, through Hezbollah, for IRGC proxies like al-Qaeda and the Taliban. Iran’s Supreme Leader and central government are aware of and encourage those acts. Applying pressure against the United States by funding and supplying Hezbollah and other terrorist proxies is an official component of IRGC policy.

105. The Qods Force provides weapons, funding, and training for terrorist operations targeting American citizens in Afghanistan, including by supporting terrorist organizations such as the Taliban. *See, e.g., Cabrera at *36.* As the U.S. government’s Joint Improvised Explosive

Device Defeat Organization (“JIEDDO”) concluded in a 2009 report: “Iran’s use of weapons smuggling networks is fairly predictable and meant to shape the manner in which foreign countries deal with Iran.” For that reason, the Qods Force varies the quantity, rate, and types of weapons provided to its proxy terrorist organizations depending on the amount of pressure Iran wants to exert on a particular country.

106. The Qods Force operates a broad global network of front companies, often co-located with Hezbollah. The IRGC created the Qods Force’s Unit 400, which was tasked with facilitating the IRGC’s terrorist finance and logistics activities through illicit commercial transactions conducted by a global network of IRGC fronts.

107. In October 2007, the U.S. Treasury Department designated the Qods Force as a Specially Designated Global Terrorist (“SDGT”) under Executive Order 13224 for providing material support to the Taliban and other terrorist organizations, including Hezbollah and terrorist groups in Iraq.²² Treasury also designated multiple Qods Force members as Specially Designated Nationals pursuant to Executive Order 13224, based on their activities in Afghanistan. *Id.* Announcing the Qods Force’s SDGT-related designations, Treasury confirmed that “[t]he Qods Force”:

- (i) “provide[d] material support to the Taliban, Lebanese Hizballah, Hamas, [and] Palestinian Islamic Jihad”;
- (ii) “[was] the [IRGC’s] primary instrument for providing lethal support to the Taliban”;
- (iii) “provide[ed] weapons and financial support to the Taliban to support anti-U.S. and anti-Coalition activity in Afghanistan”;
- (iv) “support[ed] Hizballah’s military, paramilitary, and terrorist activities, providing it with guidance, funding, weapons, intelligence, and logistical support”;

²² Press Release, *U.S. Treasury Dep’t, Fact Sheet: Designation of Iranian Entities and Individuals for Proliferation Activities and Support for Terrorism* (Oct. 25, 2007).

- (v) “operate[d] training camps for Hizballah in Lebanon” “and” “trained more than 3,000 Hizballah fighters at IRGC training facilities in Iran”;
- (vi) “provide[d] roughly \$100 to \$200 million in funding a year to Hizballah and” “assisted Hizballah in rearming in violation of UN Security Council Resolution 1701”; and
- (vii) “provide[d] lethal support in the form of weapons, training, funding, and guidance to select groups of Iraqi Shi’a militants who target[ed] and kill[ed] Coalition [] forces.” *Id.*

108. Considering the foregoing, the Treasury Department confirmed, on behalf of the U.S. government, that “[t]hrough Qods Force material support” the United States “believe[d] Iran [was] seeking to inflict casualties on U.S.” “forces” in the Middle East. *Id.*

109. Moreover, the Treasury Department emphasized that the U.S. government intended the Qods Force’s newly announced SDGT designation to signal to multinational corporations and their C-Suites – like Defendants – that they could no longer do business with the IRGC’s commercial fronts. Among other things, Treasury stated:

- (i) “The U.S. Government is taking [] major actions today to counter Iran’s ... support for terrorism by exposing Iranian ... companies and individuals that have been involved in these dangerous activities and by cutting them off from the U.S. financial system....”
- (ii) “Last week, [] Treasury [] issued a warning to U.S. banks setting forth the risks posed by Iran.... Today’s actions are consistent with this warning, and provide additional information to help [] institutions protect themselves from deceptive [] practices by Iranian entities and individuals engaged in or supporting ... terrorism.”
- (iii) “As a result of our actions today, all transactions involving any of the designees and any U.S. person will be prohibited ... Today’s designations also notify the international private sector of the dangers of doing business with ... the many IRGC-affiliated companies that pervade several basic Iranian industries. ...”
- (iv) “Support for Terrorism -- Executive Order 13224 Designations E.O. 13224 is an authority aimed at freezing the assets of terrorists and their supporters, and at isolating them from the U.S. financial and commercial systems.” *Id.*

110. The U.S. Department of State designated the Qods Force as an FTO in April 2019, along with the IRGC.

II. HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC LED A CONSPIRACY TO ACCOMPLISH THEIR “SECURITY” MISSION OF EXPELLING THE UNITED STATES FROM THE MIDDLE EAST

111. Given the complexity of Defendants’ participation in the IRGC Conspiracy as alleged in this Complaint, Plaintiffs first outline the Conspiracy’s structure, before proceeding to set forth detailed allegations regarding the same.

112. In this section, Plaintiffs identify: (A) the object of the Conspiracy; (B) the parties to the Conspiracy; (C) how the attacks that occurred in this case were acts in furtherance of the Conspiracy; and (D) the dates on which we think each Defendant joined the Conspiracy and the manner by which they joined the Conspiracy.

A. The Object Of The Conspiracy And Its Leadership

113. The IRGC established the IRGC Conspiracy after 9/11 and it continued, with respect to Afghanistan, until the end of the terrorist campaign in Afghanistan. Today, the IRGC Conspiracy continues wherever Americans are present in the Middle East, and the IRGC continues to sponsor attacks against Americans in furtherance of the Conspiracy.

114. The “IRGC Shareholders” who organized the Conspiracy comprised the three constituent parts of the IRGC, i.e., the IRGC’s Hezbollah Division, the IRGC’s Qods Force, and the Regular IRGC (hereinafter, the “IRGC Shareholders”).²³

115. The Object of the IRGC Conspiracy was for the IRGC Shareholders to accomplish their “security” mission of expelling the United States from the Middle East.

²³ The IRGC Shareholders are one and the same with the Iranian Shareholders, defined above, because the Iranian Shareholders were merely fronts for the IRGC Shareholders.

116. On information and belief, at all relevant times, each of the three IRGC Shareholders made a roughly co-equal contribution to the Conspiracy with respect to funds, equipment, weapons, terrorist personnel, technologies, and logistics.

117. **The IRGC's Hezbollah Division** has the same meaning as Hezbollah, and was one of the leaders of the Conspiracy:

- (i) **Role:** Hezbollah was a designated FTO based upon its role as the IRGC's External Security Organization, meaning, its service as the IRGC's lead agent for conducting "External Security" operations (i.e., anti-American terrorism) worldwide. As the IRGC's "security" proxy specialist worldwide, Hezbollah was tasked with organizing anti-American "resistance" attack campaigns to aid the Afghanistan Terror Campaign and Iraq/Syria Terror Campaign (as defined below) in furtherance of the Conspiracy.
- (ii) **Leadership:** Hezbollah was commanded by **Hassan Nasrallah** ("Nasrallah"), who was notorious (as covered by the media) internationally and in Iran for being a terrorist, and, on information and belief, understood by each Defendant to be an IRGC terrorist who commanded some of the largest IRGC terrorist finance, logistics, communications, weapons, narcotics, and operations fronts. Nasrallah did all of this to aid the Afghanistan Terror Campaign and Iraq/Syria Terror Campaign in furtherance of the Conspiracy.

118. **The IRGC's Qods Force** is the IRGC's Iranian-staffed external "Security" Operations Division, which at all relevant times worked closely with Hezbollah.

- (i) **Role:** The Qods Force was a designated SDGT based upon its service as the IRGC's Iranian-nationality external terror organization that is the flip side of Hezbollah's External Security Organization and designed to work with Hezbollah through the IRGC's joint cell approach. The Qods Force served alongside Hezbollah as the IRGC's "security" proxy specialist worldwide and, as such, was tasked, alongside Hezbollah, with organizing anti-American "resistance" attack campaigns to aid the Afghanistan Terror Campaign and Iraq/Syria Terror Campaign in furtherance of the Conspiracy.
- (ii) **Leadership:** Until his death in 2020, the Qods Force was commanded by **Brigadier General Qassem Soleimani** ("Soleimani"), who was notorious (as covered by the media) internationally and in Iran for being a terrorist, and, on information and belief, understood by each Defendant to be an IRGC terrorist who served as the head of the Qods Force and commanded some of the largest IRGC terrorist finance, logistics, communications, weapons, narcotics, and operations fronts, and worked closely with Hezbollah pursuant to the IRGC's joint cell model. Soleimani did all of this to aid the Afghanistan Terror Campaign and Iraq/Syria Terror Campaign in furtherance of the Conspiracy.

119. **Regular IRGC** is the IRGC's Internal Security Division (hereinafter as an organization, "Regular IRGC," and as individual members, "IRGC Regulars").

- (i) **Role:** Regular IRGC and the IRGC Regulars operated *exclusively* within Iran and served primarily as fronts for IRGC's terrorist finance, logistics, illicit technology acquisition, and intelligence activities, to coordinate the logistics and supply chain needs for Hezbollah and Qods Force, through Regular IRGC's fronts and cover companies, charities, and foundations inside Iran, including, but not limited to, the Bonyad Mostazafan, IEI, IEDC, and TCI. Regular IRGC did all of this to aid the Afghanistan Terror Campaign and Iraq/Syria Terror Campaign in furtherance of the Conspiracy.
- (ii) **Leadership:** Regular IRGC was commanded by the IRGC terrorist, **IRGC Chief of Staff Mohammad Forouzandeh** ("Forouzandeh"), who was notorious (as covered by the media) internationally and in Iran for being a terrorist, and, on information and belief, understood by each Defendant to be an IRGC terrorist who served as the IRGC Chief of Staff and commanded the largest IRGC terrorist finance, logistics, and operations front, the Bonyad Mostazafan.²⁴ Forouzandeh did all of this to aid the Afghanistan Terror Campaign and Iraq/Syria Terror Campaign in furtherance of the Conspiracy.

120. To accomplish the object of the Conspiracy, the IRGC recruited additional terrorist groups, corporate partners, criminal organizations, and individuals to aid the IRGC's global campaign terrorizing Americans through coordinated terrorist violence facilitated by the IRGC Shareholders in order to conduct IRGC "resistance" operations, i.e., anti-American terrorist attacks, in furtherance of the Conspiracy (such joining person, a "Member" of the Conspiracy). Each Member regularly provided valuable "**Security Aid**" (as defined below), to facilitate attacks that aided the Iraq/Syria Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy. Each Member's actions were to aid the Iraq/Syria Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

121. Each Member who joined the Conspiracy had to pledge that they would provide significant aid to help the IRGC Shareholders support their "security" operations, by directly or

²⁴ Forouzandeh effectively midwived the Qods Force. He was appointed to be chief of staff of the IRGC in order to reorganize it to suit the Ayatollah's needs. A few years into his tenure, also at Khomeini's direction, Forouzandeh oversaw the formal creation of the Qods Force in 1990.

indirectly facilitating one or more of the following flows of material support from the Defendants and/or the United States as a result of the Defendant's conduct, to flow through the Defendant or another entity whom the Defendant owned or otherwise controlled, before reaching the persons who committed the attacks that killed and injured Plaintiffs.

122. Each Member facilitated the provision of one or more of the following forms of "Security Aid" to the IRGC (inclusive of each of its IRGC Shareholders) and the Haqqani Network (an FTO and Member of the Conspiracy): (a) fundraising to finance terrorist operations, including "tax" collection and diaspora donations, including *khums*; (b) logistics; (c) attack planning; (d) assassinations and bombings (design and execution); (e) illicit technology acquisition; (f) Big Data analytics and management; (g) operations; (h) communications; (i) transport; (j) narcotics trafficking; (k) smuggling; and (l) intelligence operations (each, a form of "Security Aid").

123. Each form of Security Aid materially assisted the Members' ability to commit attacks to aid the Afghanistan Terror Campaign in furtherance of the Conspiracy.

124. Each Member Provided Security Aid To Other Members Of The Conspiracy To Aid The Iraq/Syria Terror Campaign And Afghanistan Terror Campaign in furtherance of the Conspiracy.

B. The Parties To The Conspiracy

1. FTO/SDGT Co-Conspirators

125. Hezbollah, the Qods Force, and Regular IRGC started the Conspiracy and led it throughout. As to one or more Plaintiffs,²⁵ the FTO Co-Conspirators include Hezbollah, al-Qaeda (including its Syrian branch, ANF), and the Haqqani Network. (The Taliban, of which

²⁵ The FTOs common to all Plaintiffs are Hezbollah and al-Qaeda.

the Haqqani Network is a part, is an SDGT.) Each FTO/SDGT Co-Conspirator's actions were to aid the Iraq/Syria Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy. The Taliban joined the Conspiracy alongside its Haqqani Network and agreed to facilitate attacks to aid the Iraq/Syria Terror Campaign on or about 2005, and the Afghanistan Terror Campaign on or about 2006.²⁶

2. Corporate Front Co-Conspirators

126. The corporate fronts or "covers" for the IRGC, who joined the Conspiracy were: (1) MTN Irancell; (2) TCI and MCI; and (3) Exit40. Discovery will likely reveal additional Corporate Front Co-Conspirators.

i. MTN Irancell

127. MTN Irancell is a joint venture between MTN Group, which has a 49% stake and is not in charge, and the Bonyad Mostazafan and Iran Electronics Industries ("IEI"), which collectively own a 51% stake and are fronts for Hezbollah, the Qods Force, and Regular IRGC. MTN Irancell is an Iranian company and its principal place of business is in Tehran, Iran.

128. MTN Irancell operates as, and MTN Irancell's employees and agents work as operatives for, a front for Hezbollah, the Qods Force, and Regular IRGC.

129. Irancell joined the Conspiracy on or about 2004, when the IRGC seized Irancell in order to convert it into an instrument of terrorism, and Irancell remained in the Conspiracy after officially becoming MTN Irancell in 2005.

130. MTN Irancell remained in the Conspiracy at all times since Irancell became MTN Irancell in 2005, and MTN Irancell remains in the Conspiracy today.

²⁶ For the avoidance of all doubt, Plaintiffs do not mean to suggest that these groups were not engaged in terrorist attacks prior to these dates, only that this was when these groups reached agreement with the Iranian Shareholders.

131. MTN Irancell served (and continues to serve) as an IRGC front to aid the Iraq/Syria Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

ii. MTN Group

132. MTN Group was a cover for Hezbollah, the Qods Force, and the Regular IRGC.

133. MTN Group joined the Conspiracy by no later than September 18, 2005, when MTN Group's CEO, Phuthuma Nhleko, secretly agreed that MTN Group would cause all of MTN's subsidiaries and affiliates to serve as fronts for the "Iranian Shareholders," which MTN Group's CEO knew was a direct reference to Hezbollah (an FTO) and the Qods Force. On that date, MTN Group, acting through Mr. Nhleko – on behalf of MTN Group and every MTN affiliate and subsidiary – secretly executed a letter agreement between MTN Group and MTN's "Iranian Shareholders" counterparty (i.e., the IRGC through its notorious fronts), in which MTN pledged to provide "security" assistance to the IRGC as a required condition precedent to the creation, and continuation, of MTN Irancell (the "Letter Agreement" or "Agreement"). MTN Group's Letter Agreement with Hezbollah, the Qods Force, and Regular IRGC is attached as **Exhibit A**. MTN Group and Mr. Nhleko executed the Agreement and joined the Conspiracy while physically alongside a senior IRGC officer, whom they knew to be a senior IRGC officer. During this signing, MTN Group, through Mr. Nhleko, also knew that MTN Group and the IRGC officer who countersigned on behalf of the "Iranian Shareholders" were physically consummating their agreement inside the Bonyad Mostazafan's headquarters in Tehran, Iran, while knowing that the Bonyad Mostazafan was a front designed to aid IRGC terror activities. In this agreement Letter Agreement in Tehran in the presence of one or more notorious IRGC terrorists, in which MTN Group promised to ensure that MTN Irancell aided the "security" agenda of the "Iranian Shareholders." Irancell, TCI, and MCI were also co-conspirators.

134. MTN Group's serial deceptions about the Letter Agreement demonstrate MTN's consciousness of guilt at having joined the Conspiracy.

135. Thereafter, MTN Group served as a front for the financial and procurement activities of Hezbollah (through Exit40) and all three IRGC Shareholders through their other "Security Aid" identified in the Complaint.

136. MTN Group served as an IRGC cover to aid the Iraq/Syria Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

137. MTN Group authorized the payment of, at a minimum, millions of dollars each year from 2009 through 2020 that MTN Group caused to be paid to the Haqqani Network, both before and, on information and belief, after it was designated an FTO. Each such payment or authorization by MTN Group was an act in furtherance of the Conspiracy because MTN Group knew it was paying money to an ally of the IRGC Shareholders who would use it to aid their proxy terror attacks against Americans in the Middle East. When MTN Group made or authorized such payments, it did so to aid the Iraq/Syria Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

138. MTN Group's promises to pay (in 2005) and payments (in 2007) of a \$400,000 bribe to "Short John" (an IRGC cut-out) and \$200,000 bribe to "Long John" (to corruptly swing a U.N. vote), were acts in furtherance of the Conspiracy because MTN Group knew it was paying money to an ally of the IRGC Shareholders who would use it to aid their proxy terror attacks against Americans in the Middle East. When MTN Group made or authorized such payments, it did so to aid the Iraq/Syria Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

139. MTN Group's attempts to repatriate, and repatriation of, money from Irancell using the mails and wires of the United States from 2012 through 2018 were acts in furtherance of the Conspiracy because, on information and belief, to access the money MTN Group had to also authorize a substantial financial transfer to MTN Irancell, which MTN Group knew would flow to an ally of the IRGC Shareholders to aid their proxy terror attacks against Americans in the Middle East. When MTN Group made or authorized such payments, it did so to aid the Iraq/Syria Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

iii. TCI and MCI

140. TCI and MCI were fronts for Hezbollah, the Qods Force, and the Regular IRGC.

141. TCI and MCI joined the Conspiracy on or about 2009 and remain in it today.

142. TCI and MCI served as an IRGC front to aid the Iraq/Syria Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

iv. Exit40

143. On information and belief, Exit40 is a front company owned, controlled, and operated by Hezbollah.

144. On information and belief, Exit40 was purpose-built by Hezbollah, following IRGC terrorist tradecraft, to serve as a front for illicit fundraising and acquisition of embargoed U.S. technologies including American smartphones and servers.

145. On information and belief, Exit40 supplied the described Security Aid to other Members of the Conspiracy in order to aid the Iraq/Syria Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

146. On information and belief, Exit40 joined the Conspiracy no later than on or about 2005, when MTN Group caused Exit40 to be hired as a consultant or a distributor on behalf of MTN Group, MTN Irancell, or another MTN subsidiary.

147. On information and belief, Exit40 routed tens of millions in value through MTN Group, MTN Dubai, MTN Irancell or another MTN entity, which was all done at the direction of MTN Group, and which flowed the value to Hezbollah from 2005 until on or about 2012. Hezbollah, in turn, shared such resources to facilitate attacks to aid the Iraq/Syria Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

3. Corporate Supplier and Manufacturer Co-Conspirators

148. The IRGC Conspiracy operated through its terrorist members to carry out attacks on Americans, with the IRGC providing logistical and financial support. The attacks in this case were all acts in furtherance of the IRGC Conspiracy. Every person that agreed to join the IRGC Conspiracy is therefore liable for the harm caused by these attacks.

149. Defendants MTN Group, ZTE Corp. and Defendant Huawei Co. joined the IRGC Conspiracy when they agreed with known IRGC fronts (variously including, but not limited to, MTN Irancell, TCI, MCI, and Exit40) to provide resources, technical materials, and technical support, and to support Iran's "security" objective.

150. Defendants MTN Group, ZTE Corp. and Huawei Co. agreed to provide such assistance in order to aid the Iraq/Syria Terror Campaign and Afghanistan Terror Campaign in furtherance of the IRGC Conspiracy.

151. Each of MTN Group, ZTE Corp. and Huawei Co., and each of their U.S. manufacturer co-Defendants, acted in furtherance of that agreement to join the IRGC Conspiracy each time they provided money and other resources, provided technical goods (such as cell phones and telecom infrastructure), assisted with technical support, evaded U.S. sanctions in order to do so, and attempted to obfuscate their respective roles.

152. Each time MTN, ZTE, and Huawei did these acts in furtherance of the IRGC Conspiracy, such Defendant assisted the IRGC Conspiracy's objective to attack Americans and ultimately expel the U.S. from Afghanistan and the Middle East.

C. Plaintiffs Were Injured By Attacks In Afghanistan That Occurred In Furtherance Of The Conspiracy

153. Plaintiffs were injured by attacks that were conducted in one of terrorist campaigns that the IRGC facilitated in furtherance of the IRGC Conspiracy in Afghanistan.

154. Institutional sources of illicit transnational terrorist finance in the Iraq/Syria Terror Campaign – especially narcotics trafficking – strengthened the potency of the Afghanistan Terror Campaign, and vice versa, because the Hezbollah and the Qods Force worked closely with al-Qaeda and the Taliban (including its Haqqani Network) to maximize the huge income for all involved. Such strategies produced tens of millions in cross-pollinated income streams between IRGC Shiite Terrorist Proxies and IRGC Syndicate Terrorist Proxies, which increased the flow of resources to facilitate attacks to aid the Iraq/Syria Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

1. The Iraq/Syria Terror Campaign

155. The Iraq/Syria Terror Campaign comprised terrorist attacks in Iraq and Syria from 2006 through the present that were committed by IRGC Shiite Terrorist Proxies and/or IRGC Syndicate Terrorist Proxies against Americans in Iraq and Syria for the specific purpose of inflicting pain on the United States to drive the United States out of Afghanistan and Iraq in furtherance of the IRGC Conspiracy, where the FTO or FTOs that committed the attack received material support from Hezbollah, the Qods Force, and Regular IRGC to aid such attacks against Americans in Iraq.

2. The Afghanistan Terror Campaign

156. The Afghanistan Terror Campaign comprised terrorist attacks in Afghanistan from 2007 through the present day that were committed by IRGC Shiite Terrorist Proxies and/or IRGC Syndicate Terrorist Proxies against Americans in Afghanistan to inflict pain on the United States to drive the U.S. out of Afghanistan and Iraq in furtherance of the Conspiracy, where the FTO or FTOs that committed the attack received material support from Hezbollah, the Qods Force, and Regular IRGC to aid such attacks against Americans in Afghanistan.

157. The Afghanistan Terror Campaign unfolded much in the same manner as the Iraq/Syria Terror Campaign but started about a year later (the IRGC began with Iraq before broadening to Afghanistan). In 2005, Hezbollah, the Qods Force, and the Regular IRGC helped kickstart the Afghanistan Terror Campaign. Hezbollah, the Qods Force, and the Regular IRGC did so to aid the Iraq/Syria Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

158. On or about 2006, the Taliban joined the Conspiracy. On information and belief, the Taliban, did so after a series of meetings between emissaries in Afghanistan and Iran, including, but not limited to, in Herat, Afghanistan, and Mashhad, Iran.

159. Each Plaintiff was injured in an attack committed by one or more of the above-identified designated FTOs who joined the IRGC Conspiracy and committed the attack in furtherance of the Conspiracy.

III. AFTER 9/11, HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, TALIBAN, AND AL-QAEDA JOINED AN IRGC CONSPIRACY TO DRIVE THE UNITED STATES OUT OF THE MIDDLE EAST

A. The Formation Of The Conspiracy

1. After 9/11, Hezbollah, The Qods Force, And Regular IRGC Led A Terrorist Conspiracy Targeting Americans In Afghanistan, Iraq, And Elsewhere To Inflict Pain On “The Great Satan”

160. After 9/11, the IRGC organized a transnational terrorist alliance to marshal efficiencies across terrorist groups and maximize the lethality of their terrorist campaign.

161. By 2007, under the leadership of Qassem Soleimani, Hezbollah and the Qods Force had leveraged the IRGC’s control of telecommunications front companies, and associated profits and cell phones they acquired, to organize “resistance” (i.e., terror) cells in dozens of countries on six continents. As the *Montreal Gazette* reported at the time:

Under the Ahmadinejad administration, U.S. officials said, the [IRGC] has moved increasingly into commercial operations, *earning profits* and extending its influence in Iran in areas involving big government contracts, including ... *providing cell phones*. Washington has claimed the Revolutionary Guard’s Quds Force wing is responsible for the growing flow of explosives, roadside bombs, rockets and other arms to Shiite militias in Iraq and the Taliban in Afghanistan. Quds Force has also been blamed for supporting Shiite allies such as Lebanon's Hezbollah and to such Sunni movements...²⁷

2. To Maximize The Lethality Of Their Terrorist Conspiracy, Hezbollah, The Qods Force, And Regular IRGC Provided Material Support To Every Other Member of the Conspiracy, Including Funds, Arms, Training, And Logistical Support, Which Their Co-Conspirators Used To Attack Americans in Afghanistan

162. After 9/11, Hezbollah, the Qods Force, and Regular IRGC, organized a global terrorist alliance comprised of a litany of allied Shiite and Sunni terrorist groups. Generally,

²⁷ Montreal Gazette (Canada), *What is the Revolutionary Guard?* (Aug. 16, 2007), 2007 WLNR 28659733.

such groups could be divided between, on the one hand, transnational groups which seek to attack Americans anywhere, or regional groups, which focus on a particular geography.

163. In all cases, however, the terrorists: (a) sought to attack and kill Americans to force the United States to withdraw from the Middle East, including Afghanistan and Iraq; and (b) relied upon a network of terrorist allies – an Islamist NATO – necessary to counteract the U.S.-led coalitions in Afghanistan and Iraq, which organized the world’s most powerful militaries and intelligence services to confront these terrorists.

164. Simply put, the IRGC and its terrorist co-conspirators knew they needed their own transnational alliance with all the same functionalities as NATO to successfully prosecute a global terror campaign against Americans on multiple continents for decades.

165. After 9/11, the IRGC’s Hezbollah Division and Qods Force led the IRGC’s support for the IRGC Conspiracy. With respect to the Hezbollah Division, Hezbollah’s terrorist mastermind, Imad Mugniyeh, led this effort until the U.S. and Israel killed him in 2008, after which Mugniyeh was replaced by other well-trained and experienced Hezbollah Division terrorist operatives. With respect to the Qods Force, Qassem Soleimani, led the Qods Force-related aspects of the scheme until his own death at the hands of a U.S. drone strike in 2020.

166. To operationalize the various nodes of the Conspiracy – including transnational logistics, financial relationships, arms pipelines, smuggling routes, and the like – Hezbollah and the IRGC worked hand-in-hand with each other globally (as they have since the IRGC “midwived” Hezbollah to execute the Conspiracy). Hezbollah and the Qods Force followed the same terrorist playbook worldwide, which included support of various terrorist proxy groups.

167. **IRGC Shiite Terrorist Proxies.** If Hezbollah and the Qods Force were (a) sectarian allies with the proxy terrorists (as with Shiite group Jaysh al-Mahdi); or (b) had a long-

standing alliance regardless of sect (as with Sunni terrorist groups Hamas and Palestinian Islamic Jihad), then (c) IRGC doctrine mandated that Hezbollah and the Qods Force follow the joint cell model, in which they established joint cells comprised of Hezbollah, Qods Force, and a local proxy to attack Americans in-country, or to provide logistical, weapons, operational, financial, or concealment aid to another part of the Conspiracy that targeted Americans elsewhere.

168. **IRGC Syndicate Terrorist Proxies.** If Hezbollah and the Qods Force did *not* have a decades-long alliance with the terrorist proxy and were also not sectarian allies (*i.e.*, Shiites), then they followed an approach by which Hezbollah and the Qods Force, backed by all the IRGC's money and logistics, identified Sunni terrorist groups that could serve as allies of convenience with a shared terrorist agenda targeting the United States. The IRGC terrorist proxies who joined the Conspiracy under this approach include, but are not limited to:

- (i) **al-Qaeda**, which Hezbollah and the Qods Force supported through their global network of cells with respect to their logistics, funding, transportation, and arms supply, and which they supported inside Iran, Iraq, Syria, Afghanistan, and Pakistan, through the provision of funds, safe haven, communications, and logistical support; and
- (ii) **the Taliban and its Haqqani Network**, which Hezbollah and the Qods Force supported through their global network of cells with respect to their logistics, funding, transportation, and arms supply, and which they supported inside Iran, Iraq, Afghanistan, and Pakistan, through the provision of funds, arms, training, safe haven, communications, and logistical support²⁸

(al-Qaeda, the Taliban, including its Haqqani Network, and Lashkar-e-Taiba, collectively, being the **"IRGC Syndicate Terrorist Proxies"**).

169. Hezbollah, the Qods Force, and Regular IRGC, materially aided every aspect of both the IRGC Shiite Terrorist Proxies' and the IRGC Syndicate Terrorist Proxies' terrorist

²⁸ Hezbollah, the Qods Force, al-Qaeda, and the Taliban, including its Haqqani Network, sometimes combined forces to jointly commit an attack against Americans in Afghanistan, Iraq, or another geography to which every organization could contribute or network connections.

campaigns against Americans in Afghanistan, Iraq, Yemen, Syria, Lebanon, Europe in furtherance of the Conspiracy.

170. To facilitate terrorist attacks against Americans by IRGC Shiite Terrorist Proxies and IRGC Syndicate Terrorist Proxies, Hezbollah, the Qods Force, and Regular IRGC, depended upon the large flow of money, equipment, weapons, and logistical support, as well as the “cover” provided by the corporate entity, from the complicit corporate partners, including MTN Irancell, TCI, and any corporate allies that conspired with the IRGC to create and operate these terrorist fronts.

B. In Furtherance Of The Conspiracy, Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, The Taliban, And The Members Of The Al-Qaeda-Taliban Terrorist Syndicate Waged A Deadly Terrorist Campaign Against Americans In Afghanistan

171. The IRGC’s support of terrorist proxies like Hezbollah, Hamas, the Taliban, and al-Qaeda is well-documented.²⁹ The IRGC has also long provided material support to the Syndicate, including al-Qaeda and the Taliban. *See, e.g., Cabrera* at *1, *6, *10-11, *40. The sectarian differences between the Shiite regime in Tehran and the Sunni al-Qaeda/Taliban leadership have not hindered cooperation between the groups. Whatever their religious differences, both groups share a hatred of the United States and support anti-American violence.

172. While Americans worked to rebuild post-war Afghanistan, they were attacked by a Syndicate led by Taliban and al-Qaeda terrorists. *See, e.g., Cabrera* at *1, *6. Hezbollah, the Qods Force, and Regular IRGC, sponsored those terrorist attacks to undermine American foreign policy in Afghanistan. To that end, Hezbollah, the Qods Force, and Regular IRGC, supported the Taliban, including its most radical part, the Haqqani Network, by, among other things,

²⁹ *See* Alireza Nader, Joya Laha, *Iran’s Balancing Act in Afghanistan* at 9 (RAND Corp. 2011) (“*Iran’s Balancing Act*”).

training Taliban terrorists how to attack Americans effectively and paying terrorists who killed U.S. forces. Hezbollah, the Qods Force, and Regular IRGC also provided the Taliban with sophisticated weapons that it used to kill and injure thousands of Americans.

173. The IRGC's, including Hezbollah's and the Qods Force's, support for al-Qaeda was equally potent. *See, e.g., Cabrera* at *10. That decades-long support has included money, weapons, training, logistical assistance, and safe harbor for al-Qaeda leaders. In 2007, Osama bin Laden himself referred to Iran as al-Qaeda's "main artery for funds, personnel, and communication." The IRGC's, including Hezbollah's and the Qods Force's, decision to back al-Qaeda despite sectarian differences reflected Iran's overriding desire to foment global anti-American terrorism. That decision, like the one to support the Taliban, paid dividends. The IRGC's, including Hezbollah's and the Qods Force's, support for al-Qaeda in Afghanistan substantially contributed to the terrorist violence that killed and injured Americans there.

174. The IRGC's, including Hezbollah's and the Qods Force's, support for al-Qaeda complemented its support for the Taliban because of the close relationship between the two terrorist groups. *See, e.g., Cabrera* at *10. Although al-Qaeda and the Taliban were nominally separate groups, they acted together in a terrorist "Syndicate" that planned and authorized terrorist violence throughout Afghanistan. *See, e.g., Cabrera* at *1, *6. That Syndicate – which involved mafia-style meetings between leaders of the Syndicate's various members – provided a superstructure that organized and facilitated a range of terrorist attacks in Afghanistan. By funneling material support to multiple members of that Syndicate, Hezbollah, the Qods Force, and Regular IRGC ensured that the IRGC's policy of sponsoring anti-American terrorism in Afghanistan achieved maximum effect. *See, e.g., Cabrera* at *10.

175. After 9/11, Hezbollah and the Qods Force operationalized a sophisticated pipeline for routing material support to al-Qaeda and the Taliban to facilitate attacks against Americans in Afghanistan through which the IRGC supplied al-Qaeda and the Taliban with the communications technologies, including cell phones, and taught their use as terrorist weapons. Indeed, in 2012, the U.K. government publicly accused the IRGC of transferring mobile phones to Taliban terrorists targeting Coalition forces in Afghanistan, and also accused the IRGC of training Taliban terrorists how to deploy such IRGC-provided mobile phones to improve the lethality and effectiveness of the Conspiracy's IED attacks targeting Americans in Afghanistan:

- (i) "Iranian bomb makers are suspected of being behind the device which killed the six soldiers." ... "Funded partly by the Taliban, the [Iranian] instructors have taught insurgents in Helmand to disguise bombs from electronic detection, producing a bigger and more deadly blast."
- (ii) "Intelligence experts believe Iran is increasingly influencing the style and impact of attacks against ... [NATO] troops in southern Afghanistan." ... "... the Iranians ... are suspected of teaching the bomb makers involved the techniques needed to avoid roadside counter-measures."
- (iii) "Border officials in Herat, a city on Afghanistan's western border with Iran, have reported that a wide range of material made in Iran—including mortars, plastic explosives, propaganda materials *and mobile phones*—is also ending up in insurgents' hands. And a Taliban commander admitted that the insurgents had grown more dependent on Iran ..."
- (iv) "[T]he Iranians have taught Taliban fighters to link mobile phones to the bomb, allowing the trigger man to watch for a suitable target before he strikes. ... [The Taliban's IED] techniques have become increasingly sophisticated, intelligence officials say, under the influence of the Iranians."³⁰

176. The IRGC Conspiracy succeeded. The U.S. substantially completed its withdrawal from Afghanistan on or about August 2021, which was one of the four primary objects of the Conspiracy. Afghanistan was also, along with Iraq, one of the two central theaters

³⁰ See, e.g., David Williams, *The Iran Connection: How Taliban Learned To Make Undetectable Bombs*, Daily Mail (Mar. 8, 2012), 2012 WLNR 5017775.

where both Hezbollah, the Qods Force, and Regular IRGC, and the IRGC's Sunni allies al-Qaeda and the Taliban, regularly collaborated in a two-way manner, sharing resources, personnel, smuggling routes, financiers (in-country and around the world), and sometimes even jointly committing attacks with one another.

177. Plaintiffs identify below several terrorist groups, subgroups, and partnerships responsible for the specific attacks that killed and injured them. Each worked in concert and shared resources, personnel, and operational plans. Indeed, the Taliban and al-Qaeda often participated in mafia-style meetings – attended by the leaders of several allied terrorist groups – in which they planned and authorized various terrorist attacks throughout Afghanistan.³¹ Given such coordination, one former CIA official and senior White House advisor called the resulting terrorist superstructure a “Syndicate,” composed of al-Qaeda, the Taliban, and several allied FTOs.³² In fact, bin Laden himself conceived of al-Qaeda as the leader of a broader coalition of terrorists drawing from other terrorist organizations in Pakistan and Afghanistan.³³

178. Iran's support for multiple components of this “Syndicate” ensured that its support had maximum effect. Due to the mutually reinforcing ties between the Taliban and al-Qaeda in Afghanistan, support for the one benefited the other – and vice versa. Iran recognized those interrelationships and so spread its support across multiple parts of the Afghan terror Syndicate. In doing so, Iran was able to achieve its intended effect: wide-ranging terrorist

³¹ See Bill Roggio and Thomas Joscelyn, *The al Qaeda – Taliban Connection*, Wash. Exam'r (July 4, 2011) (“*The al Qaeda-Taliban Connection*”), archived at <https://www.washingtonexaminer.com/weekly-standard/the-al-qaeda-taliban-connection>.

³² Bruce Riedel, *Deadly Embrace: Pakistan, America, And The Future Of The Global Jihad* at 1 (Brookings Inst. Press 2d ed. 2011).

³³ *The al Qaeda-Taliban Connection*.

attacks against Americans, executed mostly by the Taliban but supported by (and sometimes jointly committed with) al-Qaeda and the other components of the Syndicate.

179. Against that backdrop, Plaintiffs identify below the principal Afghan terrorist groups, subgroups, and cells that committed the attacks that killed and injured them. Plaintiffs also identify how Hezbollah, the Qods Force, and Regular IRGC, facilitated terrorist attacks by al-Qaeda, the Taliban (including its Haqqani Network), and their allies.

1. Al-Qaeda

180. Since its inception, al-Qaeda doctrine has emphasized terrorist strategy that borrows heavily from cooperative game theory principles, including concepts such as cooperation theory, franchising, and joint ventures. “Since the September 11, 2001 terrorist attacks, al Qaeda emerged as the head of a global Islamist terror movement, comprised of dozens of deadly jihadist groups” and “[s]everal members of the al Qaeda terror movement [were] designated as FTOs” including, but not limited to, “Islamic Movement of Uzbekistan,” “Jaish-e-Mohammed,” and “Lashkar-e-Tayyiba.”³⁴ This reflected al-Qaeda’s tactical and operational fusion with its affiliates in Afghanistan and Pakistan.

181. Since 9/11, and continuing through the present, Al-Qaeda led the Syndicate and worked jointly with its inseparable ally, the Taliban, with whom al-Qaeda had been essentially fused since before 9/11 and has remained so ever since. The overlap between the organizations meant that al-Qaeda often played a key role in Taliban and Haqqani Network attacks. As terrorism scholars Bill Roggio and Thomas Joscelyn observed, “[i]t is not clear where, say, al Qaeda ends and the Taliban and other terrorist groups begin. This is by design. Bin Laden

³⁴ Jimmy Gurulé, *Unfunding Terror: The Legal Response to the Financing of Global Terrorism* 89 (Edward Elgar 2008) (hereinafter, “Gurulé, *Unfunding Terror*” or “Gurulé”).

envisioned al Qaeda as the vanguard of a broader jihadist coalition. Al Qaeda was always a joint venture.”³⁵ Mr. Joscelyn testified that the word “syndicate” – referring to al-Qaeda’s terrorist joint venture with its Afghan and Pakistani affiliates – offers an “excellent description of how al Qaeda operates.”³⁶

182. The U.S. State Department designated al-Qaeda as an FTO on October 8, 1999.

183. Al-Qaeda’s and the Taliban’s close relationship continued long after 9/11. In the years since, it has become clear that the al-Qaeda and Taliban organizations have been fused together: al-Qaeda terrorists have often worked in close conjunction with Taliban terrorists and the affiliated Haqqani Network and Kabul Attack Network. In May 2007, Taliban official Mullah Dadullah said, “[W]e and al-Qaeda are as one.”³⁷ In early 2009, a military intelligence official was quoted as saying, “The line between the Taliban and al Qaeda is increasingly blurred, especially from a command and control perspective.”³⁸ By the end of that year, Chairman of the Joint Chiefs of Staff Admiral Michael Mullen said the same thing openly. “We are deeply concerned about the growing level of collusion between the Taliban and al Qaeda,” he told *The Wall Street Journal*.³⁹ And as Lieutenant General Ronald L. Burgess, Jr. stated in a February 2010 Hearing of the Senate Select Committee on Intelligence, “al Qaeda’s propaganda, attack planning and support of the Taliban and Haqqani networks continues.”

³⁵ *The al Qaeda – Taliban Connection*.

³⁶ *Al-Qaeda In Afghanistan and Pakistan: An Enduring Threat*, Hr’g Before the U.S. House Committee On Foreign Affairs, Subcommittee On Terrorism, Nonproliferation, and Trade, S. Hr’g 113-156, at 28 (May 20, 2014) (statement of Thomas Joscelyn, Sr. Research Fellow, Found. for Def. of Democracies), 2014 WLNR 13518260.

³⁷ Thomas Ruttig, *The Other Side* 23, Afghanistan Analysts Network (July 2009).

³⁸ Bill Roggio, *Al Qaeda Builds A ‘Shadow Army’*, Wash. Times (Feb. 13, 2009).

³⁹ Anand Gopal, *Afghan Police Killings Highlight Holes in Security*, Wall St. J. (Dec. 15, 2009).

184. By 2009, al-Qaeda and the Haqqani Network intensified their attack campaign inside Afghanistan. To do so, they ramped up their terrorist finance campaigns worldwide, putting out a call to all al-Qaeda and Haqqani Network financiers to support the jihad against Americans in Afghanistan the same way both groups had previously rallied terrorist financiers worldwide to support the campaign against the Soviets in the 1980s.

185. Thereafter, due in large part to the Syndicate's terrorist finance, al-Qaeda's terrorist campaign grew more lethal each month and year.

186. Al-Qaeda's Syndicate-counterattack-strategy reflected bin Laden's long-standing vision of al-Qaeda (and himself, specifically) as the leader of a grand terrorist coalition across Afghanistan and Pakistan. Due to the mutually reinforcing ties between al-Qaeda, the Taliban (including its Haqqani Network), and Lashkar-e-Taiba in Afghanistan – including their practice of cross-donations to each other – support for one benefited all. Defendants' support to the Syndicate's terrorist finance and bombmaking logistics thus had crosscutting effects: they enabled wide-ranging terrorist attacks against Americans in Afghanistan.

187. Al-Qaeda's leadership of that terrorist Syndicate reflected the degree to which al-Qaeda and the Taliban became fully and operationally intertwined. As India's Permanent Representative to the United Nations explained on October 1, 2011 in describing the al-Qaeda-Taliban "syndicate of terrorism," both groups were by 2011 "ideologically and operationally fused." By the fall of 2009, noted journalist Peter Bergen publicly stated, "the Taliban and Al Qaeda function more or less as a single entity. The signs of this are everywhere."⁴⁰

⁴⁰ Peter Bergen, *The Front: The Taliban-Al Qaeda Merger*, New Republic (Oct. 19, 2009) ("The Front").

188. Internationally, al-Qaeda and the Haqqani Network (and through it, the Taliban) shared intertwined streams for finance, logistics, smuggling, and weapons. According to Haqqani Network expert Gretchen Peters, international “funding streams” were “intertwined across” amongst al-Qaeda, the Haqqani Network, and the Taliban.⁴¹ As Ms. Peters explained in 2012, al-Qaeda, the Haqqani Network, and their allies “derive[d] income in and outside Afghanistan” and their “money move[d] between key network actors and into banks in Pakistan, the [U.A.E.] and beyond.”⁴²

189. The Taliban and al-Qaeda have remained intimately intertwined. For example, in 2015, Osama bin Laden’s successor, Ayman Zawahiri, pledged an oath of allegiance to the recently-installed Taliban leader Mullah Akhtar Mohammad Mansour, who publicly announced his acceptance of the pledge the following day. When Mansour was killed in May 2016, Zawahiri pledged allegiance to his successor, Mawlawi Haibatullah Akhundzada.

190. Often, individual Taliban leaders are also members of al-Qaeda. For example, in late 2011 or early 2012 the Taliban appointed Sheikh Mohammed Aminullah, who has close ties to al-Qaeda, as the head of its Peshawar Regional Military Shura, which is responsible for attacks in northern and eastern Afghanistan.

191. Al-Qaeda also encouraged the Taliban to embrace new terrorist techniques. In February 2003, bin Laden issued a recording calling specifically for suicide attacks in Afghanistan and Iraq. Taliban terrorists had previously viewed suicide attacks as taboo, but al-Qaeda convinced them they were religiously permissible. Indeed, al-Qaeda trumpeted their ideological success online, announcing, “While suicide attacks were not accepted in the Afghani

⁴¹ Gretchen Peters, *Haqqani Network Financing: The Evolution Of An Industry* 32, Combatting Terrorism Ctr. (July 2012) (“Peters, *Haqqani Network Financing*”).

⁴² *Id.*

culture in the past, they have now become a regular phenomenon!” With al-Qaeda’s encouragement and training, the number of such suicide attacks in Afghanistan increased from one in 2002, two in 2003, and six in 2004, to 21 in 2005 and more than 100 in 2006. Al-Qaeda further encouraged these attacks by paying the families of suicide bombers in Afghanistan.

192. Al-Qaeda’s role in that suicide-bombing trend was pivotal. As Islamic history scholar Bryan Glyn Williams explained, “Al Qaeda operatives carried out two to three [suicide] bombings per year on the Afghan government and NATO troops from 2002 to 2004 that were meant to demonstrate the effectiveness of this alien tactic to the local Taliban. These demonstrative acts and videos of successful [Al Qaeda] suicide bombings in Iraq seem to have convinced the Taliban to condone the previously taboo tactic of suicide bombing.”⁴³

193. Al-Qaeda operatives also served as embedded trainers with Taliban forces. These experienced trainers provided instructions, funding, and resources for conducting local and international attacks. By 2005 at the latest, al-Qaeda began bringing instructors from Iraq to train the Taliban how to fight Americans. For example, al-Qaeda members trained Taliban commanders in bomb-making techniques. Al-Qaeda also invited Taliban commanders to Iraq, where they learned how to make armor-penetrating “shaped” charges,⁴⁴ a type of IED later known as an EFP. Taliban trainees also learned how to use remote controls and timers, and urban warfare tactics.

⁴³ Bryan Glyn Williams, *Afghanistan Declassified: A Guide to America’s Longest War* at 202 (Univ. Penn. Press 2012).

⁴⁴ Sami Yousafzai, *Unholy Allies*, Newsweek (Sept. 25, 2005).

194. As one writer put it in November 2009, “[s]mall numbers of Al Qaeda instructors embedded with much larger Taliban units have functioned something like U.S. Special Forces do – as trainers and force multipliers.”⁴⁵

195. According to a declassified 2008 Defense Intelligence Agency intelligence report, by the mid-2000s, al-Qaeda’s partnership with the Haqqani Network had facilitated the emergence of a Sirajuddin Haqqani-led network of al-Qaeda training camps in Waziristan.⁴⁶

196. Al-Qaeda has also established multiple training camps within Afghanistan reportedly hosted by the Taliban. One such camp covered nearly 30 square miles and contained heavy weapons, IED-making material, anti-aircraft weapons, rocket-propelled grenade systems, machine guns, pistols, rifles, and ammunition.

197. On top of the myriad forms of support detailed above, al-Qaeda also jointly planned and authorized terrorist attacks that the Taliban carried out. Those joint planning sessions often occurred in meetings in which al-Qaeda, the Taliban, and other members of the al-Qaeda-Taliban Syndicate (such as Lashkar-e-Taiba) would confer about particular geographies and targets to attack. The close operational coordination not only manifested itself in the Kabul Attack Network, but also provided a broader terrorist superstructure that organized the insurgency throughout Afghanistan. In observing in 2011 that this superstructure formed an Afghan-Pakistani “Syndicate” of sorts, a former CIA analyst and White House advisor documented several notable Syndicate-sponsored attacks in Afghanistan that “demonstrated the

⁴⁵ Peter Bergen, *The Front*, New Republic (Oct. 19, 2009), <https://tinyurl.com/zutk7x9k>.

⁴⁶ Def. Intel. Agency, *Location and Activities of the Training Centers Affiliated with the Haqqani Network, Taliban, and al-Qaeda in Northern Waziristan and Future Plans and Activities of Sarajuddin ((Haqqani))*, Intel. Information Report (Apr. 16, 2008), <https://tinyurl.com/2ed3a2b4>.

intricate connections between al Qaeda and its allies in Pakistan and Afghanistan.” Those intimate connections enhanced the lethality of the overall anti-American insurgency.

198. Information derived from al-Qaeda and Taliban detainees held at Guantanamo Bay, Cuba (“Gitmo”) corroborates the planning and authorization activities of the al-Qaeda-Taliban Syndicate. For example, according to purported Gitmo intelligence files quoted by terrorism experts Bill Roggio and Thomas Joscelyn (*Al-Qaeda-Taliban Connection, supra*), one detainee, Abdul Razak, was a “high-level military commander in a newly-conceived ‘unification’ of Al Qaeda, [Hezb-e-Islami Gulbuddin (“HIG”),] and Taliban forces within Afghanistan,” which the leaders of the respective terrorist groups “envisioned [as a] new coalition of HIG, Al Qaeda, and Taliban during a meeting in Pakistan in early spring 2003.”. Another purported detainee file quoted by Messrs. Roggio and Joscelyn concerning Haroon al Afghani, a dual-hatted al-Qaeda/HIG terrorist, contained the following intelligence report:

[Afghani] is assessed to have attended a joint operations meeting among extremist elements in mid-2006. A letter describing an 11 August 2006 meeting between commanders of the Taliban, al Qaeda, [Lashkar e Taiba], . . . and the Islamic Party (probably a reference to the HIG), disclosed that the groups decided to increase terrorist operations in the Kapisa, Kunar, Laghman, and Nangarhar provinces, including suicide bombings, mines, and assassinations. (*Id.*)

199. Taken together, these reports “demonstrate a high degree of collusion between al Qaeda and other terrorist groups” as part of a “jihadist hydra” that shares the “common goal” of seeking to “drive the U.S.-led coalition out of Afghanistan.” *Id.* One al-Qaeda operative, whom U.S. officials characterized as “an important al-Qaida planner and explosives expert,” Ghazwan al-Yemeni, trained Taliban members in Pakistan. He eventually helped plan the December 30, 2009 attack on Camp Chapman that killed seven Americans.

200. Al-Qaeda doctrine emphasized the development and deployment of dual- or even triple-hatted terrorists, whom counter-terror and counter-narcotics professionals describe as

“polyterrorists” (or “poly-traffickers”). Al-Qaeda fashioned itself into a multinational corporation for Islamist terrorists, and therefore embraced an aggressive expansion strategy in the late 1990s, which accelerated even more after 9/11, in which al-Qaeda scaled up by making other terrorist groups into its new partners. Al-Qaeda’s doctrines concerning cooperation with other jihadists and the need for interoperability substantially mirrors that of Hezbollah, the Qods Force, and Regular IRGC. As a result, al-Qaeda, and its star pupil, the Taliban, often relied upon joint cell tactics to carry out their most spectacular attacks.

201. Al-Qaeda terrorists also regularly attacked U.S. forces alongside Taliban terrorists, including in some of the attacks that killed or injured Americans. For example, in the early 2000s, al-Qaeda’s third-ranking member participated in attacks on Americans in Afghanistan alongside Taliban terrorists under the command of Sirajuddin Haqqani. As another example, on July 13, 2008, Taliban and al-Qaeda members jointly attacked a U.S.-Afghan outpost in Nuristan Province. Nine NATO ISAF (International Security Force Afghanistan) soldiers were killed in the attack.

202. In 2010, a terrorism scholar warned against drawing a bright line between al-Qaeda and the Afghan terrorist groups that it sponsored. In explaining the importance of “recogniz[ing] the link between al-Qa’ida and Afghan insurgent groups,” he observed that a “policy focused on targeting al-Qa’ida – and not the Taliban, Haqqani Network, or other groups – would ignore one of the most egregious lessons from September 11.”⁴⁷

⁴⁷ Seth G. Jones, *In the Graveyard of Empires: America’s War in Afghanistan* at 332 (W.W. Norton & Co. 2010) (“*Graveyard of Empires*”).

203. The U.S. government agreed. During the relevant timeframe, the U.S. government repeatedly stated that al-Qaeda and the Taliban acted together in a terrorist “syndicate,” and warned against efforts to distinguish between them. Examples include:

- (i) Secretary of State Hillary Clinton, July 2009: “[A]l-Qaeda is supported by and uses its extremist allies like . . . the Taliban . . . to be proxies for a lot of its attacks . . . So the Taliban . . . [is] part of a kind of terrorist syndicate with al-Qaeda at the center[.]”⁴⁸
- (ii) Secretary of State Hillary Clinton, December 2009: “[W]e have increasingly come to see these organizations not as separate independent operators that occasionally cooperate with one another, but as part of a syndicate of terrorism. . . . And at the head of the table, like an old Mafia kind of diagram, sits al Qaeda.”⁴⁹
- (iii) Secretary of Defense Robert Gates, January 2010: “Defense Secretary Robert M. Gates said yesterday that Al Qaeda was using proxy terrorist groups to orchestrate attacks in . . . Afghanistan as part of a broader strategy to destabilize the region. In a news conference . . . Gates said Al Qaeda had formed a ‘syndicate’ of terrorist groups with Taliban factions in Afghanistan and Pakistan . . . US intelligence officials have said that jihadi groups in the region are cooperating more closely than ever . . . Gates said all of the factions were working under the umbrella of Al Qaeda.”⁵⁰
- (iv) Secretary of Defense Robert Gates, May 2010: “The other concern we have . . . is the creation of the syndicate of terrorist organizations that are working with each other, al Qaeda, the Taliban in Pakistan, the Taliban in Afghanistan, the Haqqani Network. There are five or six of these groups that are now really working together and a success for one is a success for all.”⁵¹
- (v) Under Secretary of Defense Michele Flournoy, April 2011: “We view al Qaeda, Haqqani, the Taliban, these are all part of a syndicate of groups that help each other.”⁵²

204. Al-Qaeda’s interdependence and joint venture with its affiliates in Afghanistan and Pakistan continued throughout the period in which Plaintiffs were killed and injured. As two journalists noted in 2016, the U.S. military’s relative success against al-Qaeda neither eliminated

⁴⁸ *Sec. of State Hillary Clinton*, NBC News: Meet the Press (July 26, 2009).

⁴⁹ S. Hr’g 111-479, at 24.

⁵⁰ *Gates Casts Qaeda As Terror Syndicate*, Wash. Post (Jan. 21, 2010), 2010 WLNR 1263055 (“*Gates Casts Qaeda As Terror Syndicate*”).

⁵¹ *John King Presents: Full Interview with Secretary of Defense Robert Gates*, CNN (May 8, 2010), 2010 WLNR 27823364.

⁵² *Hindustan Times, Pakistan Must Meet Certain Expectations on Counter-Terrorism* (Apr. 22, 2011).

al-Qaeda nor broke apart its Syndicate: Afghanistan's southern and eastern provinces remained a "hub of Afghan insurgents and [the] al-Qaeda-led terrorist syndicate."⁵³ Similarly, as two terrorism scholars explained in a 2018 book, "[t]he Taliban still retain[ed] a close alliance with al-Qaeda," which represented "the worst possible scenario for terrorism."⁵⁴

205. Today, Afghanistan is a safe haven for al-Qaeda under the control of the "Islamic Emirate of Afghanistan." The Taliban promised U.S. negotiators that they would sever their alliance with al-Qaeda and kick them out of Afghanistan. That was a lie, and they have done the exact opposite since their victory. Indeed, al-Qaeda's continuing fusion with the Taliban, was amply demonstrated after the fall of the U.S.-allied government there to the terrorists, when a litany of high-level al-Qaeda terrorists publicly traveled back to their ancestral haunts in Afghanistan, media retinue in tow, for the "conquering hero" photo-op.

2. Sirajuddin Haqqani (Al-Qaeda and Taliban)

206. From 9/11 through today, al-Qaeda's terrorist enterprise benefited from al-Qaeda operatives who were "polyterrorists," *i.e.*, al-Qaeda terrorist operatives who *also* simultaneously served as a terrorist operative for one or more al-Qaeda affiliates. By design, al-Qaeda operatives were often members of other Pakistan-based al-Qaeda affiliates, most commonly, the Haqqani Network and Lashkar-e-Taiba. Typically, al-Qaeda's and the Haqqani Network's

⁵³ Ayaz Ahmed & Dr. Faisal Javed, *Pakistan And SCO: Opportunities for Pakistan*, Asian Defence J. (Aug. 31, 2016), 2016 WLNR 25890108.

⁵⁴ Walter Laquer and Christopher Wall, *The Future of Terrorism* 153 (St. Martin's Press 2018) ("Laquer and Wall, *Future of Terrorism*").

polyterrorist operatives or agents served the Syndicate’s transnational terrorist activities in support of the attack campaign against Americans in Afghanistan.⁵⁵

207. Since the mid-2000s, Sirajuddin Haqqani was – and remains today – the signal example of an al-Qaeda “polyterrorist” operative who killed Americans. Sirajuddin Haqqani was the son of bin-Laden’s long-standing ally, mentor, and protector, Jalaluddin Haqqani. By 2008, Sirajuddin Haqqani was simultaneously: (1) a senior al-Qaeda operative, leader, and attack planner, who served as the most important member of al-Qaeda’s military council (essentially, its terrorist planning committee); (2) the Haqqani Network’s top operative, attack planner, and leader; and (3) a senior leader of the Quetta Shura Taliban, which would eventually make him its number two leader (Deputy Emir). *See, e.g., Cabrera at *Sirajuddin’s unparalleled biography and personal networks made him the hub of al-Qaeda and Taliban terror.*

208. On February 29, 2008, the U.S. State Department designated Sirajuddin Haqqani a SDGT for “acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy, or economy of the United States” and the U.S. Congress specifically identified Sirajuddin Haqqani as “the overall leader of the Haqqani Network as well as the leader of the Taliban’s Mira shah Regional Military Shura” in 2012.⁵⁶

⁵⁵ *See, e.g., Juan C. Zarate, Treasury’s War: The Unleashing of a New Era of Financial Warfare* 41 (Public Affairs 2013) (Treasury’s [counter-terror] strategy ... aimed at targeting networks of key financial actors and nodes in the terrorist support system. The point was ... to make it harder for individuals who were financing terrorists to access the formal financial system. Our analyses therefore focused on the networks of actors and institutions providing the financial backbone to terrorist enterprises. Interestingly, we found that there were all-purpose financiers who would give to multiple causes—‘polyterror’ supporters.”) (“Zarate, *Treasury’s War*”).

⁵⁶ Public Notice, *In the Matter of the Designation of Sirajuddin Haqqani, aka Sirajuddin Haqqani, aka Siraj Haqqani, aka Siraj Haqqani, aka Saraj Haqqani, aka Saraj Haqqani, as a Specially Designated Global Terrorist Pursuant to Section 1(b) of Executive Order 13224, as Amended*, 73 Fed. Reg. 12,499 (Mar. 7, 2008); Pub. L. 112-168, 126 Stat. 1299, § 2(a)(8) (Aug. 10, 2012).

209. When the U.S. Treasury Department designated Sirajuddin Haqqani's uncle Khalil Al-Rahman Haqqani as a SDGT, it noted that he "has also acted on behalf of al-Qa'ida and has been linked to al-Qa'ida military operations."⁵⁷ The Treasury Department likewise has repeatedly recognized links between Haqqani Network leaders and al-Qaeda.

210. Sirajuddin Haqqani facilitated al-Qaeda members' efforts to join and fight with the Haqqani Network and the rest of the Taliban. According to U.S. intelligence officers, Sirajuddin Haqqani acts as a member of al-Qaeda's military council. U.S. officials have described him as al-Qaeda's top facilitator in Afghanistan.

211. Other than Osama bin Laden, Sirajuddin Haqqani was the single most important al-Qaeda leader since 9/11. By joining al-Qaeda management, Sirajuddin achieved a level of interoperability and cohesion between al-Qaeda and the Taliban that greatly magnified the lethality of the terrorists' campaign.

212. Sirajuddin Haqqani was also, like his father Jalaluddin Haqqani, famous for his pragmatism in defense of his extremism. Sirajuddin was willing to do deals and make trades with people, groups, and governments whom he might otherwise wish to kill—provided the deal in question made it more likely that al-Qaeda and the Taliban could kill Americans in Afghanistan.

213. Sirajuddin Haqqani was the most important transnational Syndicate leader and played a vital role in harmonizing the various strategies and tactics, as well as promoting network efficiencies. Thus, for example, if a Qods Force "security" operative needed secure

⁵⁷ Press Release, U.S. Dep't of Treasury, *Treasury Targets the Financial and Support Networks of Al Qa'ida and the Taliban, Haqqani Network Leadership* (Feb. 9, 2011).

travel into Paktika Province (a Haqqani Network stronghold), the Qods Force terrorist could contact someone from the Haqqani clan and make the necessary arrangements.

214. When Plaintiffs were attacked, Sirajuddin Haqqani, and the al-Qaeda and Taliban organizations he led, promoted deep cooperation amongst al-Qaeda, the Taliban (including its Haqqani Network), and the IRGC (including Hezbollah and the Qods Force).

215. When Plaintiffs were injured between 2012 and 2017, Sirajuddin Haqqani served as the top Syndicate “polyterrorist” responsible for coordinating key transnational-facing aspects of the Syndicate’s terrorist campaign in Afghanistan and, in coordinating with other al-Qaeda and al-Qaeda affiliate terrorists. Each of the below attack campaigns or types constituted an act of international terrorism committed by al-Qaeda and the Taliban (including its Haqqani Network) that was aided by Hezbollah, the Qods Force, and Regular IRGC.

- (i) **Kabul Attack Network Attacks.** Sirajuddin Haqqani planned and authorized the Syndicate attacks that targeted Kabul – which Sirajuddin personally viewed as a tactical priority – that were committed by joint al-Qaeda/Taliban (including Haqqani Network)/Lashkar-e-Taiba cells known as the Kabul Attack Network, including such joint cell’s IED and suicide bomb attacks in Kabul and the surrounding provinces.
- (ii) **Fertilizer Bomb Attacks.** Alongside al-Qaeda, Sirajuddin Haqqani planned and authorized al-Qaeda’s fertilizer bomb campaign, including, but not limited to, al-Qaeda’s and the Haqqani Network’s strategies to: (a) source fertilizer; (b) purchase and transport fertilizer; (c) operate al-Qaeda bombmaking factories at Sirajuddin’s personal network of joint al-Qaeda-Haqqani Network terrorist camps in Pakistan; and (d) deploy fertilizer bombs as IEDs and suicide bombs to attack Americans in Afghanistan.
- (iii) **Suicide Bomber Attacks.** Sirajuddin Haqqani planned and authorized al-Qaeda’s suicide bombing campaign, including, but not limited to, its and the Haqqani Network’s shared strategy for: (a) planning the targets for suicide bomber attacks in Afghanistan; (b) sourcing suicide bombers through al-Qaeda’s and the Haqqani Network’s long-standing allies, Lashkar-e-Taiba and Jaish-e-Mohammed; and (c) coordinating the “suicide bomber infrastructure” of camps, madrassas, ratlines, and safehouses, which relied heavily upon al-Qaeda and Haqqani Network resources and polyterrorists.
- (iv) **Kidnapping Attacks.** Sirajuddin Haqqani planned and authorized kidnappings in Kabul.

- (v) **Transnational Terrorist Finance and Logistics.** Sirajuddin Haqqani planned and authorized al-Qaeda's and the Taliban's, including its Haqqani Network's, transnational terrorist logistics, including, but not limited to: (a) al-Qaeda and the Taliban's transnational rackets necessary to the success of their: (1) criminal funding efforts, (e.g., money laundering, protection rackets, and tax fraud); (2) fundraising and money movement, e.g., diaspora donations, banking relationships; (3) "tax" collection from the criminal underworld of their diaspora globally, e.g., logistics, communications in the U.A.E., Pakistan, Afghanistan, and Europe; and (b) al-Qaeda's and the Haqqani Network's transnational-operations and activities in Afghanistan, Pakistan, and the U.A.E. as they relate to smuggling or logistics, both of which have always ranked as top Haqqani Network specialties.
- (vi) **Coordination Between FTOs.** Sirajuddin Haqqani led two FTOs (al-Qaeda and the Haqqani Network) and was responsible for, or supervised those who were responsible for (like his brother Anas) managing al-Qaeda's and the Taliban's (including its Haqqani Network's) relationships with a broad international alliance of allied terrorists, including, but not limited to: (a) Hezbollah, the Qods Force, and Regular IRGC; (b) the Pakistani Taliban, a member of the Syndicate; (c) Lashkar-e-Taiba, a member of the Syndicate; and (d) Jaish-e-Mohammed, a member of the Syndicate.

216. For more than a decade, and continuing through to today, Sirajuddin Haqqani was wanted by the FBI for his involvement in numerous acts of terror against Americans (he still is).

217. On February 20, 2020, the *New York Times* shamefully published a propaganda op-ed authored by Siraj titled "What We, the Taliban, Want."⁵⁸

218. Along with his brothers, who were also (and remain) key Haqqani Network leaders, as well as al-Qaeda operatives and/or agents, Sirajuddin Haqqani personally spearheaded the terrorists' successful campaign on Kabul in August 2021. Today, Sirajuddin Haqqani serves as the terrorist who is responsible for the "Islamic Emirate of Afghanistan's" borders and guns, while his brothers have responsibilities relevant to intelligence and information.

3. The Taliban

219. The Taliban is a Sunni Islamist terrorist organization comprised originally of former mujahideen fighters who had expelled the Soviet Union from Afghanistan. The Haqqani

⁵⁸ Sirajuddin Haqqani, *What We, the Taliban, Want*, N.Y. Times (Feb. 20, 2020).

Network is the most radical part of the Taliban. While Plaintiffs address each separately, they are part of the same organization (i.e., the Taliban). *Cabrera* at *8.

220. On July 3, 2002, the U.S. designated the Taliban and leader Omar as SDGTs. President Bush found that these designations guarded against “grave acts of terrorism and threats of terrorism committed by foreign terrorists.”

221. On December 26, 2007, Congress enacted a law declaring that, for purposes of “section 212(a)(3)(B) of the Immigration and Nationality Act, . . . the Taliban shall be considered to be a terrorist organization.”⁵⁹ As a State Department official explained, the U.S. government treats the Taliban “as a Foreign Terrorist Organization for immigration purposes.”⁶⁰

222. At all relevant times, the U.S. government viewed the Taliban as a terrorist group, not as the legitimate armed force of any nation.

223. The Taliban’s principal goal has long been to expel Americans from the country and undermine the democratically elected government of Afghanistan. To that end, the Taliban attacked U.S. forces from 2001 through 2020, and achieved its objective in 2021.

224. The Taliban used threats of terrorist violence to extract protection money from international companies doing business in Afghanistan. Such threats were particularly frequent in (though not limited to) geographic areas of Taliban control. By 2006, the Taliban had achieved control of wide swaths of southern and eastern Afghanistan, and by 2009 it had installed “shadow” governments in 33 of Afghanistan’s 34 provinces. It leveraged that control into protection payments. As an anticorruption investigator working for the U.S. House of Representatives explained in 2010, it was “long-standing business practice within Afghanistan to

⁵⁹ Consolidated Appropriations Act of 2007, § 691(d), Pub. L. No. 110-161.

⁶⁰ U.S. Dep’t of State, *Senior Administration Officials on the Terrorist Designation of the Haqqani Network* (Sept. 7, 2012).

use your control of the security environment in order to extort payment from those who want to operate within your space, whether it's construction of a cellphone tower, a dam, or running trucks.”⁶¹ The Taliban perfected that practice by threatening contractors' businesses until (and sometimes even after) they met the terrorists' financial demands.

225. The Taliban's threats presented companies with a choice: alert the government and seek the U.S. military's assistance while investing in legitimate security to protect their projects, or instead save time and money by paying the Taliban to direct its attacks elsewhere. One American executive whose company conducted business in Afghanistan described the decision as “‘whether you'd rather pay \$1,000' for Afghans to safely deliver a truck, even if part of the money goes to the insurgents, or pay 10 times that much for security provided by the U.S. military or contractors.’”⁶² Companies, including Defendants, typically chose the former option. The owner of one logistics subcontractor described the prevailing mentality: “‘I pay the Taliban not to attack my goods, and I don't care what they do with the money,’ he said laughing. ‘If you don't, the next day your property is attacked and destroyed.’”⁶³

226. Companies, including Defendants, rationalized their payments to the Taliban by framing them as a necessary cost of business. But the payments were unnecessary – even from the standpoint of Defendants' own security needs – and counterproductive. In reality, they chose to pay not because of any reconstruction imperative, but because it served their financial interests. As an adviser to the Afghan Interior Ministry explained, “the costs of enabling the

⁶¹ Karen DeYoung, *Afghan Corruption: How To Follow The Money?*, Wash. Post (Mar. 29, 2010) (“*Afghan Corruption*”), 2010 WLNR 26719956.

⁶² *Id.*

⁶³ Hamid Shalizi, *Afghan Firms Said To Pay Off Taliban With Foreign Cash*, Reuters (Oct. 13, 2010) (“*Afghan Firms Pay Off Taliban*”).

Taliban's protection racket outweigh the benefits of any reconstruction that might come out of it."⁶⁴ He noted that "it might be more convenient to pay off the Taliban, and it might be faster," but it "both prolongs the war and feeds criminality, which in turn turns more people against the government."⁶⁵ By diverting money to insurgents, the payments lowered the projects' quality and undermined whatever counterinsurgency benefits they might have otherwise delivered.

227. The Haqqani Network is a Sunni Islamist terrorist organization that has been operating in Afghanistan since the 1970s. It was founded by Jalaluddin Haqqani and is now led by his son, Sirajuddin Haqqani. The Haqqani Network is a member of the Syndicate, has been a part of the Taliban for decades, and is closely allied and interdependent with al-Qaeda.

228. On September 19, 2012, the U.S. State Department designated the Haqqani Network as an FTO.

229. The U.S. designated multiple Haqqani leaders as SDGTs. As previously mentioned, the U.S. designated Sirajuddin Haqqani as an SDGT in 2008 and, in 2010 and 2011, followed up by designating three other Haqqanis—Nasiruddin, Khalil Al-Rahman, and Badruddin—as fundraisers and commanders of the Haqqani Network. By February 2014, the U.S. had designated fourteen leaders in the Haqqani Network under Executive Order 13224.

230. The Haqqani Network was especially active in the southeastern parts of Afghanistan, particularly in the Paktia, Paktika, and Khost ("P2K") Provinces. It also developed a significant presence in the surrounding Provinces of Kabul, Logar, Wardak, Ghazni, and Zabul. Because of the Haqqani Network's longstanding tribal connections to the southeastern region of Afghanistan, the Taliban often acts through the Haqqani Network in those areas.

⁶⁴ Aryn Baker, *How The Taliban Thrives* at 51, Time Magazine (Sept. 7, 2009) ("*How The Taliban Thrives*").

⁶⁵ *Id.* at 51.

231. The Haqqani Network's influence is not limited to one Afghan region. There is significant overlap between the broader leadership of the Taliban and the Haqqani Network. Sirajuddin Haqqani has been a member of the Taliban's governing council since at least 2010. Since 2015, he has been the Deputy Emir of the Taliban, the Taliban's second in command. Working alongside al-Qaeda, the Haqqani Network has overseen the Taliban's terrorist attacks on U.S. and Coalition forces in Afghanistan. For example, after September 11, Jalaluddin Haqqani effectively served as the Taliban's secretary of terrorism and planned many of the Taliban's attacks on U.S. forces in the early days following the overthrow of the Taliban government while sheltering al-Qaeda leadership at the time.

232. The Haqqani Network has significant links to al-Qaeda, dating back to the 1980s when Osama bin Laden established a training camp for his nascent terrorist group in Haqqani-controlled territory. After September 11, the Haqqanis provided sanctuary to bin Laden.

233. The Haqqani Network's close relationship with al-Qaeda and other terrorist groups has helped grow the modern terrorist Syndicate operating in Afghanistan. In furtherance of that goal, the Haqqani Network provides protection to al-Qaeda so that it can launch attacks in Afghanistan and plan acts of international terrorism abroad. Senior Haqqani Network officials also have publicly indicated that the Haqqani Network and al-Qaeda are one. And in July 2008, Jalaluddin Haqqani's son—18-year-old Muhamman Omar Haqqani—was killed alongside a top al-Qaeda commander in southeast Afghanistan. The Haqqani Network also maintains training camps and safehouses that have been used by al-Qaeda and Taliban operatives.

234. The Haqqani Network ordinarily managed the Taliban's transnational terrorist finance and logistics operations and often aided al-Qaeda's as well. When doing so, the Haqqani Network used its network of agents, operatives, and fronts in the U.A.E. as an asset for its fellow

Syndicate terrorists. The Treasury Department determined that the Haqqani Network regularly used its transnational terrorist finance activities to fund multiple al-Qaeda-affiliated Syndicate members simultaneously. For example, on February 9, 2011, the Treasury Department designated Syndicate operatives, Said Jan Abd Al-Salam and Khalil Al-Rahman Haqqani (Jalaluddin's brother), as SDGTs to "target the financial and support networks of al-Qa'ida, the Taliban and the Haqqani Network leadership."⁶⁶

235. Along with al-Qaeda, the Haqqani Network jointly operated and conducted al-Qaeda's CAN fertilizer bomb campaign in Afghanistan, and Haqqani Network agents, operatives, and fronts, including Haqqani Network co-conspirators Fatima and Pakarab, were vital to sourcing every component necessary for the Syndicate to execute its CAN fertilizer bomb campaign at a nationwide scale. By 2010, CAN fertilizer sourced from Pakistan was "one of the most coveted substances in a Taliban bomb-maker's arsenal" and served as "the basic ingredient of the Taliban's roadside bombs,"⁶⁷ and the Syndicate had developed a sophisticated end-to-end logistics chain for the sourcing, manufacture, and distribution of al-Qaeda CAN fertilizer bombs. By 2011, "U.S. military officials believe[d] the Haqqani [N]etwork" was "working closely with [CAN fertilizer] suppliers," e.g., Fatima, "to help smuggle the fertilizer across the border."⁶⁸ By the time it was designated as an FTO on September 19, 2012, the Haqqani Network, working closely with al-Qaeda, had grown and refined the Syndicate's CAN fertilizer bomb logistics chain for more than five years.

⁶⁶ *Id.*

⁶⁷ Alex Rodriguez, *Bribes Keep Taliban Flush with Explosives*, L.A. Times (May 8, 2010), 2010 WLNR 9039604.

⁶⁸ Aamer Madhani, *Tensions With Pakistan Rise Over Bomb Ingredient*, National Journal Daily (Jul. 6, 2011), 2011 WLNR 13371684.

4. The Kabul Attack Network

236. The Kabul Attack Network was an operational manifestation of the terrorist Syndicate led by al-Qaeda and the Taliban. Specifically, the Kabul Attack Network was a set of terrorist cells, which included members from each of the terrorist groups involved in the Syndicate and focused on attacks against targets in Kabul and extending outward into the provinces of Logar, Wardak, Nangarhar, Kapisa, Kunar, Ghazni, and Zabul. It was active around key waypoints and transit routes on the way to Kabul, including Wardak, Ghazni City, and areas of Logar Province.

237. The Kabul Attack Network's forward deployed terrorists were drawn from joint cells comprised of al-Qaeda, the Taliban (including its Haqqani Network), Lashkar-e-Taiba, and Jaish-e-Mohammed, each of whom participated in Kabul Attack Network attacks and contributed personnel and resources to such attacks. For each group, the Kabul Attack Network's attacks were among the most important priorities of the Syndicate's entire terrorist campaign since 9/11, and thus received special focus from each Syndicate member. By the same token, funding for any of the involved terrorist groups contributed to the Network's attacks.

238. The Kabul Attack Network was responsible for high profile and/or mass casualty attacks on Americans in Kabul and the surrounding areas that relied upon fertilizer bombs, suicide bombers, kidnappers, or insider attacks. Indeed, on January 24, 2010, the Afghan government accused al-Qaeda of specifically planning the Kabul Attack Network's CAN fertilizer bomb attacks in Kabul, which the Syndicate delivered via IED and suicide bomb.

239. Sirajuddin Haqqani, the dual-hatted al-Qaeda-Taliban terrorist, planned and authorized every attack committed by the Kabul Attack Network, working with local commanders like Mullah Dawood. to execute the Kabul Attack Network's attacks. As a result, the Kabul Attack Network's attacks were planned and authorized by at least one FTO (al-

Qaeda), and after September 19, 2012, Kabul Attack Network attacks were planned and authorized jointly by two FTOs (al-Qaeda and the Haqqani Network). As ISAF stated in 2010, the “Haqqani Network [was] deeply entrenched in the Kabul Attack Network specifically with the facilitation of weapons and fighters into the area south of Kabul in Logar and Wardak.”

240. The Kabul Attack Network’s attacks were funded and logistically supported by al-Qaeda, the Taliban (including its Haqqani Network), Lashkar-e-Taiba, and Jaish-e-Mohammed access to terrorist finance in Afghanistan, Pakistan, and worldwide, including through their Conspiracy with Hezbollah, the Qods Force, and Regular IRGC. Thus, terrorist finance that flowed to any of these groups aided Kabul Attack Network attacks.

C. In Furtherance Of The Conspiracy, The IRGC, Including Its Hezbollah Division And Qods Force, Al-Qaeda, Al-Qaeda-in-Iraq, And al-Nusra Front Waged A Deadly Terrorist Campaign Against Americans In Iraq And Syria

241. From 2003 through 2013, the IRGC provided vital aid to al-Qaeda, including its branches in Iraq and Syria, to facilitate al-Qaeda’s attacks against Americans there. The IRGC’s aid extended directly to al-Qaeda-in-Iraq (“AQI”) and its progeny, al-Nusra Front (“ANF”).

242. Through the “sinister genius” of IRGC terrorist mastermind Qassem Soleimani, the IRGC supported Sunni terrorist attacks against Americans in Iraq. This insurgency was led by a litany of IRGC assets, including the top two Sunni leaders of the Iraqi terrorism campaign: Saif al-Adel, al-Qaeda’s military chief who coordinated its campaign, including support for al-Qaeda-in-Iraq, from his Qods Force-provided safe haven in Iran, and Abu Musab al-Zarqawi, the al-Qaeda operative who led al-Qaeda-in-Iraq on the ground and co-led Ansar al-Islam with Mullah Krekar, another IRGC asset. Al-Qaeda, al-Qaeda-in-Iraq, and Ansar al-Islam, between them, accounted for essentially all Sunni terrorist attacks on Americans in Iraq from 2004 through the present, with AQI ultimately becoming ISIS. The thread running through all Iranian strategy was that, as one

analyst explained, “Iran would do everything it could to ensure that America’s experiment [in Iraq] turned into a smoldering failure.”⁶⁹

243. Throughout, it is likely that Qassem Soleimani’s support of Shiite and Sunni terrorists in Iraq and Syria collectively accounted for more Americans killed or injured in terrorist violence after 9/11 than any other single terrorist. As Karim Sadjadpour of the Carnegie Endowment for International Peace explained in an interview, given Soleimani’s support for anti-American terror,

That’s why you have ... one, if not two, generations of American military forces whom if you were to ask them, who is your worst adversary in the world, the person you see as the greatest threat to the United States? Even when Osama bin Laden was living and Baghdadi [the leader of ISIS] was living, they would have still said Qassem Soleimani.⁷⁰

244. The IRGC’s multi-faceted support for Sunni terrorists in Iraq and Syria is consistent with bin Laden’s “grand alliance” approach to anti-American terror. In fact, bin Laden himself portrayed al-Qaeda as the leader of a broader coalition drawing from other terrorist organizations in Pakistan and Afghanistan and supported by a latticework of jihadist affiliates and allies around the world.⁷¹

245. The IRGC’s support for multiple components of bin Laden’s “syndicate” ensured that its support for Sunni terrorist groups had maximum effect. Due to the mutually reinforcing ties between the IRGC, al-Qaeda, AQI, and ANF, support for any one benefited the others – and vice versa.

⁶⁹ Karim Sadjadpour, *The Sinister Genius of Qassem Soleimani*, Wall St. J. (Jan. 10, 2020) (“Sadjadpour, *Sinister Genius*”).

⁷⁰ Karim Sadjadpour, *quoted in* National Public Radio, *‘Throughline’: The Origins Of Iran’s Gen. Qassem Soleimani* (Jan. 30, 2020) (“NPR, *Throughline*”).

⁷¹ *The al Qaeda-Taliban Connection*.

246. The IRGC recognized those interrelationships and so spread its support across multiple Sunni terrorist groups targeting Americans in Iraq. In doing so, the IRGC was able to achieve its intended effect: wide-ranging terrorist attacks against Americans, executed mostly by the Sunni terrorist group AQI (inclusive of ANF), but supported by (and sometimes jointly committed with) other Iranian terrorist allies (*e.g.*, AQI (inclusive of ANF) jointly committing a suicide bombing attack with al-Qaeda).

247. Like the IRGC's use of Shiite proxies, the IRGC's use of Sunni proxies was consistent with Iran's twin strategic goals: to impose maximum terrorist violence against Americans in Iraq while simultaneously maintaining "plausible deniability" by reducing the public Iranian role inside Iraq and Syria. Rather than openly engage in armed conflict with the U.S. or other Coalition Forces, the IRGC usually attempted to present an Iraqi face to its efforts to undermine U.S. peacekeeping efforts by supporting terrorism and sectarian violence there.

248. From 2003 through the present, the IRGC was responsible for increasingly lethal attacks on U.S. forces in Iraq and Syria and, as one example, provided Sunni terrorist proxies with the capability to assemble explosives designed to defeat armored vehicles.

249. Against that backdrop, Plaintiff Matthew Schrier identify below the principal Iraqi and Syrian terrorist groups that committed the attack that injured him.

1. Al-Qaeda

250. Starting in 2002, al-Qaeda and its affiliated clerics began calling for jihad against the United States in the event of an American invasion of Iraq. For example, al-Qaeda terrorist "thought leader" Abu Qatada publicly boasted to international media that al-Qaeda and its affiliates would launch a jihad against Americans and their Iraqi allies just as al-Qaeda had launched a similar jihad against America and its Afghan allies following the U.S. invasion of Afghanistan

after 9/11, and stated: “The growth of American tyranny ... and its plan to attack Iraq and establish an ‘Iraqi Karzai’ will necessitate an even fiercer battle.”

251. Al-Qaeda’s leaders messaged to its terrorists and sympathizers that the American presence in Iraq was an American “plot” to kickstart a religious war between Sunnis and Shiites to divide the Muslim world so that the “Crusaders” (the United States) and “Jews” (Israel) could divide and conquer it.

252. Following the U.S. invasion of Iraq, al-Qaeda escalated its support for the Sunni terrorist insurgency in Iraq from its safe havens in Iran, Afghanistan, and Pakistan. For example, on March 24, 2004, an al-Qaeda spokesman issued a call for Muslims “to take part in jihad against the United States in Iraq.” Demonstrating how the Sunni groups worked together on their shared jihad against Americans in Iraq, Ansar al-Islam’s website widely repeated al-Qaeda’s message.

253. By the mid-2000s, al-Qaeda’s partnership with the Haqqani Network – a part of the Taliban that was a long-standing ally of al-Qaeda in Pakistan and Afghanistan, and that also received material support from Iran – had facilitated the emergence of a network of al-Qaeda training camps in North Waziristan, Pakistan, near the Afghan-Pakistan border, less than a week’s overland travel to Iran. According to a declassified 2008 Defense Intelligence Agency intelligence report:

[Sirajuddin] Haqqani is also affiliated with the several foreign fighter (ff) training facilities that are controlled by or associated with al Qaeda (AQ) in North Waziristan. . . . A list and brief description of each facility follows . . .

Mohammad Taher ((Yuldashov)), leader of the Islamic Movement of Uzbekistan (IMU), and his 60 bodyguards are staying at an AQ training center in Miram Shah Dand.

There is an al-Qaeda training center located at the Miskeen and Khaisur in Miram Shah. Approximately 45 U/I Arabs and Uzbeks receive training there.

An AQ training facility called “Shaki Massod” is located in Miram Shah and over 200 AQ members (NFI) reside there; Usama bin Laden has been seen in this center (NFI).

Another AQ training facility is located at Spin-Qamar in Masood District of Northern Waziristan. Over 80 Arabs receive training there (NFI).⁷²

254. Al-Qaeda also established multiple training camps within Afghanistan reportedly “hosted by the Taliban.”⁷³ One such camp covered nearly 30 square miles and contained heavy weapons, IED-making material, anti-aircraft weapons, rocket-propelled grenade systems, machine guns, pistols, rifles, and ammunition. Al-Qaeda used these camps, in part, to help run what amounted to a “continuing education” program for senior terrorist commanders and operatives that provided instruction in the above-described al-Qaeda camps in Afghanistan and Pakistan for operations against Americans in Iraq.

255. Al-Qaeda forward deployed a significant number of operatives and planners into Iraq, who were often dual-hatted terrorists who served as members of both al-Qaeda and al-Qaeda-in-Iraq. Most famously, Zarqawi was a dual-member, serving as both a member of al-Qaeda as well as the founder and leader of al-Qaeda-in-Iraq. Al-Qaeda-forward-deployed terrorists in Iraq were essential force multipliers for al-Qaeda-in-Iraq’s terrorist campaign against Americans there. Al-Qaeda operatives served in a similar role as American Green Berets, helping to “train the trainer” and scale up AQI’s terrorist capabilities.

256. Through al-Qaeda’s use of training camps in Afghanistan and Pakistan – which al-Qaeda, al-Qaeda-in-Iraq, and al-Nusra Front all accessed through the terrorist land bridge provided

⁷² Defense Intelligence Agency, *Location and Activities of the Training Centers Affiliated with the Haqqani Network, Taliban, and al-Qaeda in Northern Waziristan and Future Plans and Activities of Sarajuddin ((Haqqani))*, Intelligence Information Report (Apr. 16, 2008).

⁷³ Thomas Joscelyn and Bill Roggio, *Trump’s Bad Deal With The Taliban*, Politico (Mar. 18, 2019).

by the IRGC – terrorists from all three groups obtained the training, technical expertise, and indoctrination essential to executing the signature al-Qaeda attack types used by all three groups in Iraq, including suicide bombings, improvised explosive devices (or “IEDs”) derived from fertilizer, and attacks against helicopters. Al-Qaeda thus helped its Iraqi and Syrian branches, including al-Qaeda-in-Iraq and al-Nusra Front, bring its signature tactics to the Iraqi and Syrian theaters. They proved highly effective at countering American defenses.

257. Al-Qaeda training and expertise, in combination with that of the IRGC, was also essential to the successful adaptation of sophisticated IED types and attack strategies by Sunni terrorists in Iraq and Syria. Al-Qaeda developed sophisticated techniques for refining fertilizer into ammonium nitrate, marrying the ammonium nitrate with a lethal triggering device and delivery system, and training terrorists how to move, deploy, and maximize the lethality of the resulting fertilizer bombs, which were delivered via IED or suicide bomber. As Senator Charles Schumer stated in 2004, “truck bombs using [calcium ammonium nitrate (“CAN”) fertilizer] are the weapon of choice of al-Qaida.”

258. At all relevant times, al-Qaeda was the world leader amongst Sunni terrorist groups with respect to building sophisticated bombs, including through the process of converting CAN fertilizer into bombs to attack Western targets, having used the technique in every major area of operations for al-Qaeda-affiliated terrorists since 9/11, including, but not limited to, attacks in Indonesia, Turkey, Syria, Yemen, Iraq, Afghanistan, and Pakistan. After 9/11, al-Qaeda supported fertilizer-based bomb strategies in every theater in which it engaged in terrorist attacks against America and its allies. As one journalist wrote in 2007, “[i]n the new age of Islamist terrorism,

[CAN] fertilizer packed into a truck with plastic explosive as a detonator has also become an al Qaida trademark.”⁷⁴

259. Al-Qaeda regularly instructed terrorist operatives from its Iraqi affiliates, in person (at camps in Afghanistan, Pakistan, and Iran) and in writing, regarding CAN fertilizer bombs. For example, a 39-page al-Qaeda memo recovered from an al-Qaeda laptop in Pakistan in 2004 instructed that military explosives were often impractical to acquire, and instructed jihadists to instead use home-made explosives, including ammonium nitrate bombs derived from CAN fertilizer.

2. Al-Qaeda-In-Iraq, Including Al-Nusra Front

260. The origins of AQI and ANF trace to Abu Musab al-Zarqawi, a Jordanian terrorist who created a training camp in Afghanistan at Osama bin Laden’s invitation. By the time of the September 11, 2001 terrorist attacks, Zarqawi had trained several thousand terrorists and established a terrorist network in Iraq, Syria, and other countries in the Middle East.

261. On or about October 15, 2004, the Secretary of State designated the Zarqawi terrorist network as a Foreign Terrorist Organization (“FTO”) under 8 U.S.C. § 1189, under the name Jama’at al-Tawhid wa’al-Jihad.⁷⁵ On or about the same day, the Secretary of State also

⁷⁴ David Barrett, *Deadly Fertiliser Bombs Used By Terrorists Worldwide*, Press Association News (Apr. 30, 2007).

Designation of Jam’at al Tawhid wa’al-Jihad, Also Known as the Monotheism and Jihad Group, Also Known as the al-Zarqawi Network, Also Known as al-Tawhid, as a Foreign Terrorist Organization Pursuant to Section 219 of the Immigration and Nationality Act, 69 Fed. Reg. 61,292, 61,292 (Oct. 15, 2004).

designated Jama'at al-Tawhid wa'al-Jihad under Executive Order No. 13,224 as a Specially Designated Global Terrorist ("SDGT").⁷⁶

262. In or around October 2004, Zarqawi formally pledged allegiance to al-Qaeda and renamed his terrorist network al-Qaeda in Iraq ("AQI"). By then, Zarqawi and his organization were among the most prominent terrorists attacking Americans in Iraq and elsewhere.

263. On December 17, 2004, the U.S. government designated al-Qaeda-in-Iraq as a Foreign Terrorist Organization, which designation it has maintained ever since.

264. A U.S. airstrike killed Zarqawi in June 2006. But AQI continued after his death as a formidable terrorist group waging a violent campaign against the United States. In 2010, a new AQI leader – Abu Bakr al-Baghdadi – took control of the AQI terrorist network. Baghdadi eventually became "the world's most-wanted terrorist chieftain," with the U.S. government at one point offering a record-breaking \$25 million bounty for his capture.

265. In early 2011, shortly after Baghdadi's emergence, Syria spiraled into civil war. Many terrorist groups and other armed factions began vying for power, precipitating a near-total breakdown in Syrian governance and other civil institutions. In August 2011, the U.N. High Commissioner for Human Rights reported "a pattern of widespread or systematic human rights violations by Syrian security and military forces, including murder, enforced disappearances, torture, deprivation of liberty, and persecution."⁷⁷

⁷⁶ Determination Pursuant to Section 1(b) of Executive Order 13224 Relating to the Designation of Jam'at al Tawhid wa'al-Jihad, Also Known as the Monotheism and Jihad Group, Also Known as the al-Zarqawi Network, Also Known as al-Tawhid, 69 Fed. Reg. 61,292, 61,292 (Oct. 15, 2004).

⁷⁷ Statement by Ms. Navi Pillay, UN High Commissioner for Human Rights to the Human Rights Council 17th Special Session on "Situation of human rights in the Syrian Arab Republic" in Geneva (Aug. 22, 2011), <https://www.ohchr.org/en/statements/2011/08/statement-ms-navi-pillay-un-high-commissioner-human-rights-human-rights-council?LangID=E&NewsID=11321>.

266. In late 2011, sensing the opportunity amid the chaos, Baghdadi sent an AQI operative, named Abu Muhammad al-Julani (also spelled al-Jawlani), to establish an AQI branch in Syria. The resulting Syrian branch was called the al-Nusrah Front (“ANF”), which Baghdadi and Julani formed officially in January 2012.

267. By the end of 2012, the U.S. government recognized ANF as AQI’s Syrian branch. In December 2012, the Secretary of State amended the FTO designation for AQI to include the following aliases: al-Nusrah Front, Jabhat al-Nusrah, Jabhet al-Nusra, The Victory Front, and Al-Nusrah Front for the People of the Levant.⁷⁸ At the time, the State Department reported that ANF had already claimed responsibility for nearly 600 terrorist attacks throughout Syria. The State Department characterized ANF as carrying out AQI’s campaign to “hijack the struggles of the Syrian people for its own malign purposes.”⁷⁹

268. At all times, al-Qaeda-in-Iraq carried out al-Qaeda’s agenda in Iraq with ruthless efficiency. Using al-Qaeda’s personnel (including Zarqawi), money, expertise, and training infrastructure, al-Qaeda-in-Iraq consolidated essentially all non-Kurdish Sunni terrorists in Iraq under one banner, led by Zarqawi and his followers.

269. Al-Qaeda and al-Qaeda-in-Iraq worked closely with one another to execute a comprehensive campaign of terrorism against Americans serving in Sunni strongholds in Iraq, including, but not limited to, Ramadi, Falluja, Mosul, and other geographies where al-Qaeda and al-Qaeda-in-Iraq had a monopoly on anti-American terror. In so doing al-Qaeda and al-Qaeda-in-Iraq aggressively pursued every signature al-Qaeda attack type: suicide bombings, IED attacks, attacks against helicopters, kidnappings, sniper attacks, and complex attacks.

⁷⁸ Amendment of the Designation of al-Qa’ida in Iraq, 77 Fed. Reg. 73,732, 73,732 (Dec. 11, 2012).

⁷⁹ Victoria Nuland, *Terrorist Designations of the al-Nusrah Front as an Alias for al-Qa’ida in Iraq* (Dec. 11, 2012), <https://2009-2017.state.gov/r/pa/prs/ps/2012/12/201759.htm>.

270. Even after being rebranded as the ISIS, the group formally known as al-Qaeda-in-Iraq continued to be an al-Qaeda affiliate until on or about 2014, when al-Qaeda and ISIS formally separated.

3. The IRGC's, Including Its Hezbollah Division's And Qods Force's, Aid to Al-Qaeda, Al-Qaeda-in-Iraq, And Al-Nusra Front Facilitated Attacks Against Americans In Iraq in Syria, Including Plaintiff Matthew Schrier

271. Iran has supported a broad coalition of anti-American terrorists in the countries bordering it, Iraq and Afghanistan, including virtually every prominent Shiite and Sunni terrorist group that has operated in Iraq since the fall of Saddam. Until his death on January 2, 2020, Qassem Soleimani masterminded Iran's support for both Shiite and Sunni Anti-American terrorists, following the simple rule that any terrorist group that (a) was targeting the United States while (b) foregoing attacks inside Iran would (c) receive weapons, funding, training, logistical support, and safe havens courtesy of the IRGC, including the Qods Force. This simple calculus has underscored Iran's terrorist agenda against America in the countries bordering Iran (Iraq and Afghanistan) for decades and continues to do so through this day.

272. As one scholar writing in the journal published by the Combating Terrorism Center at West Point summarized the evidence in 2010, "it is clear that Iran has a proven ability to commission violence inside Iraq. ... As the unclassified Iraqi government Harmony records collated by the Combating Terrorism Center at West Point illustrate, the Islamic Republic of Iran has been in the business of sponsoring Iraqi paramilitary proxies for 30 years, practically the government's entire existence."⁸⁰

⁸⁰ Knights, *The Evolution of Iran's Special Groups in Iraq*.

273. When U.S. forces arrived in Iraq, Iran's nationwide terror campaign against Americans there was assigned to the Qods Force under the command of Soleimani, who answered directly to Ayatollah Khamenei.

274. As the Congressional Research Service reported in 2007, "DOD officials reportedly captured four Iranian terrorists in July 2007 who [were] accused of smuggling explosives and personnel from Iran into Iraq," and "Iran [was] suspected of supplying Iraq insurgents with IEDs, training, and new designs and technology for explosive devices, such as 'passive infrared' electronic sensors that [were] used for triggering roadside bombs" and were "more resistant to electromagnetic countermeasures [] employed by U.S. forces."⁸¹ These findings by DOD officials accord with the reality that "[a] constant feature of Iran's policy for more than 20 years has been the importance of uninterrupted cross-border resupply for Iran's proxies in Iraq."⁸²

275. According to the U.S. State Department's 2008 Country Reports on Terrorism: "The Qods Force, an elite branch of the [IRGC], is the regime's primary mechanism for cultivating and supporting terrorists abroad. The Qods Force provided aid in the form of weapons, training, and funding to HAMAS and other Palestinian terrorist groups, Lebanese Hizballah, Iraq-based militants, and Taliban fighters in Afghanistan."⁸³

276. The First Corps of the Qods Force, one of its four regional commands, implements Iran's foreign policy in Iraq. During the relevant timeframe, the Qods Force did so largely by providing the Shiite and Sunni terrorists with material support for terrorist attacks in Iraq. The

⁸¹ Clay Wilson (Specialist in Technology and National Security), *Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures*, CRS Report for Congress, at 3 (Aug. 28, 2007).

⁸² Knights, *The Evolution of Iran's Special Groups in Iraq*.

⁸³ U.S. State Dep't, *Country Reports on Terrorism 2008* at 182-83 (Apr. 2009).

First Corps' al-Ramazan Headquarters is based across several sites in Iran's largest city (and capital), Tehran, a short trip from the border with Iraq.⁸⁴

277. Raids conducted in Iraq by the elite U.S. Joint Special Operations Command ("JSOC") also proved that the IRGC and Qods Force directly deployed their own terrorists inside Iraq to help attack Americans there and to directly participate, on occasion, in attacks themselves. For example, in a late 2006 JSOC raid in central Iraq, U.S. forces detained Mohsen Chizari, the Qods Force's head of Operations and Training, as well as the Qods Force's station chiefs for Baghdad and Dubai. In another raid in northern Iraq, U.S. forces captured five Qods Force terrorists. To counter Iran's malign activities in Iraq, JSOC bifurcated its terrorist task forces and created Task Force 16 (to hunt al-Qaeda-in-Iraq) and Task Force 17 (to hunt Shiite terrorists in Iraq). In so doing, JSOC personnel from Task Force 16 and Task Force 17 discovered that Sunni and Shiite terrorists were secretly working together. They concluded that Soleimani and the Qods Force helped al-Qaeda-in-Iraq based on the Iranian conclusion that any agent of chaos and murder in Iraq – no matter whom they were or targeted– would quicken the American exit from Iraq and therefore, on balance, advance their interests given their belief that the U.S. was their top enemy.

278. "A consistent feature of Iran's patronage has been careful efforts to spread Tehran's bets across many different horses."⁸⁵ As set forth below, Iran afforded a comprehensive program of material support to Sunni terrorists targeting Americans in Iraq, as long as such groups did not also target Iran itself.

⁸⁴ Joseph Felter & Brian Fishman, *Iranian Strategy in Iraq, Politics and "Other Means"* at 18, Combating Terrorism Center (Oct. 13, 2008).

⁸⁵ Knights, *The Evolution of Iran's Special Groups in Iraq*.

i. The IRGC, Including its Hezbollah Division and Qods Force, Provided Material Support and Resources to Sunni Terrorists Targeting Americans in Iraq, Including Al-Qaeda, Al-Qaeda-In-Iraq, and Ansar Al-Islam to Undermine the U.S. Mission There

279. Through the Qods Force, and other Iranian terrorist relationships, Iran provided material support and resources to all prominent Sunni terrorist groups targeting Americans in Iraq, supporting attacks committed directly by al-Qaeda, al-Qaeda-in-Iraq, and/or Ansar al-Islam.

280. Although there are religious differences between the Shiite Iranian regime and the Sunni terrorist organizations that targeted Americans in Iraq, those differences have not deterred Iran from supporting Sunni terrorist activities. Iran and their Sunni terrorist partners share a core geopolitical aim: to inflict mass casualties on Americans in the region. Sectarian distinctions aside, Iran has supported and funded attacks by Sunni terrorists on U.S. and allied forces in Iraq to harm the United States, including al-Qaeda, al-Qaeda-in-Iraq, and Ansar al-Islam.

281. Soleimani was ready to work with any terrorist group that could grow Iran's "axis of resistance" to the U.S., even if they were Sunnis who ordinarily opposed Iran's Shiite theocracy. As Iran expert Karim Sadjadpour of the Carnegie Endowment for International Peace explained, "[u]nder Soleimani's command, Iran became the only country in the region capable of harnessing both Shiite extremism and, at times, Sunni radicalism too."⁸⁶

[Soleimani's] sinister genius in bridging sectarian divides has given Iran an enormous asymmetric advantage over its great Sunni Arab rival in the Gulf, Saudi Arabia. All Shiite extremists are willing to fight for Iran, while most Sunni extremists—including al Qaeda and Islamic State—want to overthrow Saudi Arabia, which they see as a corrupt, impious agent of the West.

Soleimani conceived of using Sunni jihadists to fight the U.S. in much the same way that the U.S. used Sunni jihadists to fight the Soviet Union in Afghanistan in the 1980s. Iran's Shiite theocracy has managed, at times, to cooperate tactically with deadly Sunni extremist groups—including the Taliban in Afghanistan and the Palestinian groups Hamas and Palestinian Islamic Jihad—against their common

⁸⁶ Sadjadpour, *Sinister Genius*.

foes, the U.S. and Israel, even as Iran has been fighting on the front lines against the Sunni fanatics of Islamic state.⁸⁷

282. Federal judges have made similar findings. For example, in a 9/11-related case against Iran, the Honorable George B. Daniels of the United States District Court for the Southern District of New York found, as a factual matter, that:

The well-known historical religious division between Sunnis and Shi'a did not, in fact, pose an insurmountable barrier to cooperation in regard to terrorist operations by radical Islamic leaders and terrorists. Iran, which is largely Shiite, and its terrorist proxy organization, Hizballah, also Shiite, entered into an alliance with al Qaeda, which is Sunni, to work together to conduct terrorist operations against the United States during the 1990s and continuing through, and after, September 11, 2001.⁸⁸

283. According to Colin P. Clarke, a terrorism expert at the Soufan Center, “Iran uses sectarianism as a cudgel when it suits the regime, but is also willing to overlook the Sunni-Shia divide when it suits Iranian interests,” and therefore Iran’s assistance to al-Qaeda, al-Qaeda-in-Iraq, and Ansar al-Islam “would not be the first time that Iran had joined forces with Sunni militants, having supported Hamas, Palestinian Islamic Jihad and the Taliban.”⁸⁹

284. U.S. officials concurred. As one observed during the height of the Sunni insurgency: “I think it stands to reason that Iran is getting something out of this as well.”

285. The “election” of Mahmoud Ahmadinejad in 2005 only deepened Iran’s affinity with Sunni extremists who shared a common hatred of America.

286. Consistent with the alliance between Iran, Lebanese Hezbollah, and al-Qaeda, and pursuing Soleimani’s terrorist vision, Iran provided material support to the three primary Sunni

⁸⁷ *Id.*

⁸⁸ *In re Terrorist Attacks on Sept. 11, 2001*, No. 03 MDL 1570 (GBD), 2011 WL 13244047, at *12 (S.D.N.Y. Dec. 22, 2011) (findings of fact).

⁸⁹ Adam Goldman, Eric Schmitt, Farnaz Fassihi and Ronen Bergman, *Al Qaeda’s No. 2, Accused in U.S. Embassy Attacks, Was Killed in Iran*, N.Y. Times (Nov. 13, 2020).

terrorist groups that were committing attacks against Americans in Iraq: al-Qaeda, al-Qaeda-in-Iraq, and Ansar al-Islam. These groups committed attacks on their own, as well as in combination with one (or both) of the other groups. In so doing, al-Qaeda, al-Qaeda-in-Iraq, and Ansar al-Islam were part of a grand alliance of Sunni terrorists that targeted Americans in Iraq with the support of Iran.

287.

ii. Iran Provided Material Support and Resources To Al-Qaeda That Established Al-Qaeda's Capabilities Before 9/11, Prevented Al-Qaeda's Collapse After 9/11, and Ensured Al-Qaeda's Status As An Iranian Sunni Terrorist Proxy in Iraq

288.

289. Iran has long provided material support and resources to al-Qaeda. The sectarian differences between the Shiite regime in Tehran and the Sunni al-Qaeda leadership have not hindered cooperation between the groups. Whatever their religious differences, both groups share a hatred of America and support anti-American violence.

290. Iran has supported al-Qaeda's terrorist activities since the early 1990s, when Osama bin Laden lived in Sudan. As Judge Daniels found, "[i]n 1991 or 1992, discussions in Sudan between al Qaeda and Iranian operatives led to an informal agreement to cooperate in providing support for actions carried out primarily against Israel and the United States."⁹⁰ "Thereafter, senior al Qaeda operatives and trainers traveled to Iran to receive training in explosives. Osama bin Laden also sent senior aides to Iran for training with the IRGC and to Lebanon for training with Hizballah."⁹¹

⁹⁰ *In re Terrorist Attacks on Sept. 11, 2001*, 2011 WL 13244047, at *11 (findings of fact).

⁹¹ *Id.*

291. “In 1993, in a meeting in Khartoum, Sudan, arranged by Ah Mohamed, a confessed al Qaeda terrorist and trainer now in a U.S. prison, Osama bin Laden and Ayman al Zawahiri met directly with Iran’s master terrorist Imad Mughniyah and Iranian officials, including IRGC Brigadier General Mohammad Baqr Zolqadr, a multipurpose member of the Iranian terrorist structure.”⁹²

292. “At the 1993 Khartoum conference, representatives of Iran, Hizballah, and al Qaeda worked out an alliance of joint cooperation and support on terrorism.”⁹³

293. “Imad Mughniyah convinced Osama bin Laden of the effectiveness of suicide bombings in driving the U.S. out of Lebanon in the 1980s, and Mughniyah became a major connection point between Iran and al Qaeda.”⁹⁴ “Osama bin Laden had been a guerilla fighter in Afghanistan and it was Mughniyah who made bin Laden into an accomplished terrorist.”⁹⁵

294. “The 1993 meeting in Khartoum led to an ongoing series of communications, training arrangements, and operations among Iran and Hizballah and al Qaeda. Osama bin Laden sent more terrorist operatives, including Saef al Adel (who would become number 3 in al Qaeda and its top ‘military’ commander), to Hizballah training camps operated by Mughniyah and the IRGC in Lebanon and Iran. Among other tactics, Hizballah taught bin Laden’s al Qaeda operatives how to bomb large buildings, and Hizballah also gave the al Qaeda operatives training in intelligence and security.”⁹⁶

⁹² *Id.* (internal citations and quotations omitted).

⁹³ *Id.* (internal citations and quotations omitted).

⁹⁴ *Id.*

⁹⁵ *Id.* (internal citations and quotations omitted).

⁹⁶ *Id.* (internal citations and quotations omitted).

295. “Another al Qaeda group traveled to the Bekaa Valley in Lebanon to receive training in explosives from Hizballah, as well as training in intelligence and security.”⁹⁷

296. “Iran’s *Charge d’Affaires* in Khartoum, Sudan, Majid Kamal, an IRGC commander, coordinated the training expeditions; Kamal had performed the same function in Beirut, Lebanon, in the early 1980s during the formation of Hizballah.”⁹⁸

297. Under its alliance with al-Qaeda, Iran also regularly hosted Zawahiri during al-Qaeda’s formative years. As Judge Daniels previously found, “[a]s a result of the creation of this terrorist alliance, al Qaeda’s Ayman al Zawahiri repeatedly visited Tehran during the 1990s and met with officers of MOIS [Iran’s Ministry of Intelligence and Security], including chief Ali Fallahian, and Qods Force chief Ahmad Vahidi.”⁹⁹

298. “The creation of the Iran–Hizballah–al Qaeda terrorist alliance was followed by a string of terrorist strikes directly against the U.S. and its allies,” leading to the first World Trade Center attack in 1993, the Khobar Towers bombing in 1996, the African embassy bombings in 1998, the USS Cole attack in 2000, and 9/11.¹⁰⁰

299. As a result of the foregoing, Iran was the proximate and but-for cause of al-Qaeda’s embrace of suicide bombing as a tactic. Qods Force and Hezbollah agents acting at Iran’s direction originally instructed al-Qaeda in the theological, technological, and tactical aspects of suicide bombing as a terrorist strategy based upon Iran’s and Hezbollah’s own successful use of suicide bombers during Iran’s war against Iraq and during the joint Iranian/Hezbollah terrorist campaign

⁹⁷ *Id.* (internal citations and quotations omitted).

⁹⁸ *Id.* at *12 (internal citations and quotations omitted).

⁹⁹ *Id.* (internal citations and quotations omitted).

¹⁰⁰ *Id.*

against Americans in Lebanon in 1983, in which Hezbollah terrorists used suicide bombers to kill hundreds of Americans serving in Lebanon.

300. When the U.S. Department of Justice indicted Osama bin Laden for the 1998 bombings of the U.S. embassies in Kenya and Tanzania, the indictment alleged that al-Qaeda had “forged alliances” with “the government of Iran and its associated terrorist group Hezbollah [sic] for the purpose of working together against their perceived common enemies in the West, particularly the United States.”¹⁰¹ A court in this District subsequently found that Iran had caused the East Africa Embassy bombings by materially supporting al-Qaeda’s operations.¹⁰²

301. The 9/11 Commission has also confirmed that there was solid and substantial proof of Iran’s repeated willingness to support terrorist proxies targeting Americans in the Middle East, including Sunnis with whom the Iranians are normally hostile, which had been demonstrated by Iranian assistance to a litany of terrorists, including 9/11 hijackers.¹⁰³

302. After 9/11, senior al-Qaeda leadership, sheltering in Iran under the patronage and with the counsel of Qods Force operatives, explicitly modeled their post-9/11 organization and tactics on the approach of Hezbollah and the Qods Force.

303. While al-Qaeda was re-building itself in Iran after 9/11, the Iranians were busy rejecting U.S. and allied requests to stop aiding al-Qaeda. For example, on or about 2002 or 2003, Iran rejected a lawfully issued extradition request by the Jordanian government for Zarqawi on the

¹⁰¹ Indictment at 3, *United States v. Bin Laden*, No. 1:98-cr-00539-LAK (S.D.N.Y. filed Nov. 5, 1998), Dkt. 1, *available at* <https://fas.org/irp/news/1998/11/indict1.pdf>.

¹⁰² *See Owens v. Republic of Sudan*, 826 F. Supp. 2d 128, 151 (D.D.C. 2011).

¹⁰³ *See, e.g., The 9/11 Commission Report* at 60 (“[T]he evidence of Iranian involvement” in the June 1996 truck bomb attack against Americans in Khobar Tower in Saudi Arabia was “strong” and there were “also signs that al Qaeda played some role.”) (July 1, 2004); *see also id.* at 240-241 (significant Iranian transportation and logistical support for 9/11 attackers).

preposterous grounds that Zarqawi – whom the Iranians knew well – was not Jordanian but, rather, Syrian. Similarly, in a 2003 face-to-face meeting in Geneva, Switzerland, then-U.S. ambassador to Iraq Ryan Crocker implored Iranian officials to cease their support for al-Qaeda’s terrorism targeting Americans in the Persian Gulf, which request the Iranians refused. By then, al-Qaeda had demonstrated its usefulness to Iran with respect to its ability to kill Americans, and Iran was already sheltering and supporting al-Qaeda’s military leader, Saif al-Adel (who was also al-Qaeda’s manager for Zarqawi’s activities in Iraq) in his Qods Force-provided Tehran safe house.

304. The Iranians rebuffed U.S. outreach because they had already reached a secret deal with al-Qaeda. Following the 9/11 attacks on the United States and subsequent routing of Sunni terrorists in Afghanistan (including al-Qaeda) in late 2001, Iran met with senior al-Qaeda leaders who had fled Afghanistan into Iran to offer military aid to support al-Qaeda’s fight against America. Iran hosted these meetings for its al-Qaeda “guests” throughout 2001 and 2002. As part of this initial offer of support, Iran pledged to provide funds and logistical support to facilitate the development of terrorist activities targeting Americans in countries bordering Iran. While the focus at the time was on Afghanistan, all involved expected the U.S. to eventually move into Iraq and for their shared terrorist enterprise to follow us there.

305. Under this secret deal between Iran and al-Qaeda after 9/11, Iran intensified its material support for al-Qaeda’s terrorist campaign against Americans around the world. Through the secret deal between Iran and al-Qaeda and the assistance that the former provided to the latter thereafter, Iran was the proximate and but-for cause of al-Qaeda’s survival as a terrorist organization after 9/11 and the al-Qaeda linked terrorist attacks against Americans in Iraq, including Plaintiffs, that inevitably followed.

306. Osama bin Laden personally concluded that al-Qaeda would have collapsed after 2001 without the secret deal and Iran's key support for al-Qaeda in the years following 9/11, and al-Qaeda's subsequent ability to execute terrorist attacks depended upon the "artery" provided by Iran. For example, in 2007, bin Laden criticized an al-Qaeda terrorist who had been planning to strike Iran-linked targets; in a secret internal al-Qaeda communique authored by bin Laden himself, bin Laden identified the key, organization-saving assistance that Iran had been providing to al-Qaeda after 9/11, stating because of Iran's historical support for al-Qaeda's terrorist operations, Iran was al-Qaeda's "*main artery for funds, personnel, and communication.*"¹⁰⁴

307. Zawahiri also emphasized close strategic cooperation between al-Qaeda and Iran, following a pragmatic approach under which al-Qaeda focused on expanding its presence in Iran. Like bin Laden, Zawahiri agreed that al-Qaeda could not survive and thrive without the support it received from Iran. In a letter reportedly written by Zawahiri, al-Qaeda thanked Iran for the Qods Force's support in setting up al-Qaeda's terrorist network in Yemen in 2008 and stated, in effect, that al-Qaeda could not have established its franchise in Yemen without the IRGC's assistance.

308. The U.S. government has also recognized the close partnership between Iran and al-Qaeda after the secret deal between the two. In July 2011, the U.S. Treasury Department designated as SDGTs six members of al-Qaeda operating in Iran under the previously described secret agreement between Iran and al-Qaeda.¹⁰⁵ In so doing, the Treasury Department concluded that the secret deal provided that al-Qaeda terrorists "must refrain from conducting any operations

¹⁰⁴ October 18, 2007 translated letter from Osama bin Laden to Karim at 1, *Bin Laden's Bookshelf*, Office of the Director of National Intelligence (2016) (emphasis added). In March 2016, the Office of the Director of National Intelligence declassified items that had been obtained by U.S. special operators in the May 2011 raid on bin Laden's compound, including this letter. See Bin Laden's Bookshelf, Office of the Director of National Intelligence.

¹⁰⁵ Press Release, U.S. Treasury Dep't, *Treasury Targets Al-Qa'ida Funding and Support Network Using Iran as a Critical Transit Point* (July 28, 2011).

within Iranian territory and recruiting operatives inside Iran while keeping Iranian authorities informed of their activities. In return, the Government of Iran gave the Iran-based al-Qa'ida network freedom of operation and uninhibited ability to travel for extremists and their families” and permitted al-Qaeda to use Iran as a “critical transit point for funding to support [al-Qaeda’s] activities.” The Treasury Department also found that “Iran’s secret deal with al-Qa’ida” facilitated a terrorist network that “serves as the core pipeline through which al-Qa’ida moves money, facilitators and operatives from across the Middle East to South Asia.”¹⁰⁶ Indeed, al-Qaeda has honored its commitment to Iran despite its attacks on Shiite Muslims elsewhere in the Middle East.

309. The U.S. Treasury Department has repeatedly recognized the link between al-Qaeda and Iran in making SDGT designations under Executive Order 13224. In February 2012, the agency designated the Iranian Ministry of Intelligence and Security (“MOIS”) as a terrorist-sponsoring entity for, among other things, supporting al-Qaeda.¹⁰⁷ In 2014, the agency likewise designated a “key Iran-based” al-Qaeda facilitator who has “assisted extremists and operatives transiting Iran on their way into and out of Pakistan and Afghanistan.”¹⁰⁸

310. The close relationship between al-Qaeda and Iran has continued in recent years. In 2017, the U.S. State Department explained, “Since at least 2009, Iran has allowed [al-Qaeda] facilitators to operate a core facilitation pipeline through the country, enabling [al-Qaeda] to move funds and fighters to South Asia and Syria.”¹⁰⁹ It further accused Iran of remaining unwilling to

¹⁰⁶ *Id.*

¹⁰⁷ Press Release, U.S. Treasury Dep’t, *Treasury Designates Iranian Ministry of Intelligence and Security for Human Rights Abuses and Support for Terrorism* (Feb. 16, 2012).

¹⁰⁸ Press Release, U.S. Treasury Dep’t, *Treasury Targets Networks Linked To Iran* (Feb. 6, 2014).

¹⁰⁹ U.S. State Dep’t, *Country Reports on Terrorism 2016* at Iran Section (July 2017).

bring to justice or identify al-Qaeda members in its custody.¹¹⁰ The next year, the agency reaffirmed those conclusions and reiterated Iran's close relationship with al-Qaeda.¹¹¹

311. Iran also supported al-Qaeda through its proxy, Lebanese Hezbollah. As the *Washington Post* reported at the time in 2002, Iran's lead terrorist proxy, Lebanese Hezbollah, was "increasingly teaming up with al Qaeda on logistics and training for terrorist operations, according to U.S. and European intelligence officials and terrorism experts."¹¹² "The new cooperation ... includes coordination on explosives and tactics training, money laundering, weapons smuggling and acquiring forged documents, according to knowledgeable sources. This new alliance, even if informal, has greatly concerned U.S. officials in Washington and intelligence operatives abroad who believe the assets and organization of Hezbollah's formidable militant wing will enable a hobbled al Qaeda network to increase its ability to launch attacks against American targets."¹¹³

312. The "collaboration" between Iran (through Lebanese Hezbollah) and al-Qaeda "illustrate[d] what analysts [said] [was] an evolving pattern of decentralized alliances between terrorist groups and cells that share[d] enough of the same goals to find common ground: crippling the United States, and forcing the U.S. military out of the Middle East and Israel out of Palestinian territory. 'There's a convergence of objectives,' said Steven Simon, a former National Security Council terrorism expert."¹¹⁴ As the *Washington Post* reported, "[a]lthough cooperation between al Qaeda and Hezbollah may have been going on at some level for years, the U.S. war against al

¹¹⁰ *Id.*

¹¹¹ *Country Reports on Terrorism 2017* at Foreword.

¹¹² Dana Priest and Douglas Farah, *Terror Alliance Has U.S. Worried; Hezbollah, Al Qaeda Seen Joining Forces*, *Washington Post* (June 30, 2002), 2002 WLNR 15332564.

¹¹³ *Id.*

¹¹⁴ *Id.*

Qaeda [] hastened and deepened the relationship. U.S. officials believe that after al Qaeda was driven from Afghanistan, leader Osama bin Laden sanctioned his operatives to ally themselves with helpful Islamic-based groups, said a senior administration official with access to daily intelligence reports.”¹¹⁵ The *Post* concluded:

European and U.S. intelligence operatives on the ground in Africa and Asia said they have been trying to convince headquarters of the new alliances but have been rebuffed. “We have been screaming at them for more than a year now, and more since September 11th, that these guys all work together,” an overseas operative said. “What we keep hearing back is that it can’t be because al Qaeda doesn’t work that way. *That is [expletive]*. Here, on the ground, these guys all work together as long as they are Muslims. There is no other division that matters.”¹¹⁶

313. Al-Qaeda’s alliance with Iran’s lead terrorist proxy, Lebanese Hezbollah, continued at all relevant times and proved the intelligence operatives on the ground had been right all along. For example, in 2012, the Council on Foreign Relations reported that “al-Qaeda ha[d] stepped up its cooperation on logistics and training with Hezbollah, a radical, Iran-backed Lebanese militia drawn from the minority Shiite strain of Islam.”¹¹⁷

314. On or about August 7, 2020, on the anniversary of the Iran/al-Qaeda bomb attack against U.S. embassies in Africa, Israeli commandos acting at the request of the United States killed al-Qaeda’s number 2 leader, Abu Muhammad al-Masri, in a covert mission in Tehran.¹¹⁸ Masri was in Iran as a guest of the Iranian government and was permitted to freely plan attacks against the United States from an Iranian-provided safe-haven in Tehran. The timing of the attack was not a coincidence, but a rather a professional slap in the terrorists’ face extended by the U.S.

¹¹⁵ *Id.*

¹¹⁶ *Id.*

¹¹⁷ *al-Qaeda (a.k.a. al-Qaida, al-Qa`ida)*, Council on Foreign Relations (June 6, 2012).

¹¹⁸ Goldman at al., *Al Qaeda’s No. 2, Accused in U.S. Embassy Attacks, Was Killed in Iran*.

and Israeli governments to Iran and al-Qaeda, as the latter allies suffered an embarrassing and catastrophic loss on the anniversary of one of their greatest terrorist triumphs.

315. The mafia-style “syndicate” of which al-Qaeda, al-Qaeda-in-Iraq, and Ansar al-Islam formed a part, made attacks by each group more lethal. Iran’s mutually reinforcing support for al-Qaeda, AQI, and AI therefore made each group more effective.

316. By supporting al-Qaeda, Iran provided material support and resources for the extrajudicial killings that killed or injured Plaintiffs or members of their families. Al-Qaeda directly participated in many of the attacks that killed or injured Plaintiffs or their family members. Moreover, al-Qaeda was closely intertwined with al-Qaeda-in-Iraq and Ansar al-Islam and associated terrorist groups acting in Iraq, and al-Qaeda planned and authorized the Sunni attacks in which it did not directly participate. Material support and resources provided to al-Qaeda thus also flowed to al-Qaeda-in-Iraq and Ansar al-Islam, causing the injury and deaths of Plaintiffs or their family members.

iii. Iran Used the IRGC to Establish Al-Qaeda-In-Iraq as an Iranian Sunni Terrorist Proxy in Iraq

317. Iran used the IRGC to provide Zarqawi with the Iranian patronage necessary to establish al-Qaeda-in-Iraq and turn it into the terrorist killing machine it would become.

318. “When the Taliban government collapsed, a strange opportunity presented itself. Many members of al-Qaida fled Afghanistan and crossed the border into Iran.”¹¹⁹

319. All told, Zarqawi was based in Iran for at least a year after his escape from Afghanistan after 9/11. After bin Laden family members and Zarqawi joined Iran as “guests”

¹¹⁹ NPR, *Throughline*.

following 9/11, Soleimani devised a successful plan to turn them into Iranian terrorist assets to carry out attacks against America. As Mr. Sadjadpour explained:

After the U.S. military campaign to topple the Taliban began, Iran detained hundreds of al Qaeda fighters fleeing Afghanistan, including some members of Osama bin Laden's family and Abu Musab al-Zarqawi, the future leader of al Qaeda in Iraq. Many Iranians saw these jihadists as a threat—Sunni zealots who hated overwhelmingly Shiite Iran. Yet Soleimani, the architect of the Islamic Republic's plans for regional dominance, realized that they could also be an asset. ... many al Qaeda members [] spent months and even years as "guests" of Iran. Soleimani broke bread with bin Laden's sons, who affectionately called him Hajji Qassem ... He appointed two senior Quds Force officers to "provide the guests with whatever they needed," including refrigerators, widescreen TVs and an "unlimited budget" to furnish a religious library. Saif al-Adel, a notorious al Qaeda explosives expert, had access to a sports complex in a posh Tehran neighborhood, where he swam laps alongside Western diplomats.¹²⁰

320. "Now that Soleimani had these al-Qaida fighters on his side, he had to figure out exactly how to use them. And when the U.S. invaded Iraq in 2003, he saw his opening."¹²¹ As Mr. Sadjadpour of the Carnegie Endowment explained, "[i]f you're Qassem Soleimani, you think to yourself - we will do everything in our power to make sure that the U.S. war in Iraq is a colossal failure."¹²² Thus, under Soleimani's plan, Iran "unleashed the al-Qaida fighters into Iraq," doing so "[w]ith the understanding that you guys, go do what you do. Go after the United States" by deploying terrorist attacks like "car bombings, [and] suicide bombings."¹²³

321. Backed by Iran's material support, just a few months after Soleimani helped unleash him into Iraq, "Abu Musab al-Zarqawi, the Jordanian al-Qaida leader, [] set[] off these

¹²⁰ Sadjadpour, *Sinister Genius*.

¹²¹ NPR, *Throughline*.

¹²² Sadjadpour, *quoted in* NPR, *Throughline*.

¹²³ *Id.*

three major bombs which essentially destroy[ed] the American experiment in Iraq in its infancy.”¹²⁴ As terrorism scholar David Blair summarized the Zarqawi-Iran alliance:

By 2002, an Anglo-American invasion of Iraq seemed inevitable. Sensing an opportunity, Iran allowed Zarqawi to travel across its territory and enter northern Iraq in late 2002. Just as the Kaiser’s Germany transported Lenin from Switzerland to Russia in 1917 delivering him “like a plague bacillus”, in Churchill’s phrase so Iran conveyed the virus represented by Zarqawi to Iraq. The Shia rulers of Iran are natural opponents of al-Qaeda’s Sunni zealots, but the evidence suggests that the two have sometimes been tactical if mistrustful allies against a common Western enemy. So it was that al-Qaeda’s plague had arrived in Saddam Hussein’s domain, courtesy of Iran, even before the invasion. By the time that American and British tanks rolled across the Iraqi frontier in 2003, Zarqawi was already in position to organise an insurgency. Later that year, he proclaimed the birth of ‘al-Qaeda in the Land of Two Rivers’. ... From 2005 onwards, he set out to kill as many Iraqi Shias as possible[,] a bitter irony given that Zarqawi owed his very presence in Iraq to the indulgence of Shia Iran.¹²⁵

322. As a result, Iran, through Soleimani’s plan, was the proximate and but-for cause of al-Qaeda-in-Iraq’s existence and ability to commit attacks targeting Americans in Iraq, including against Plaintiffs. As Osama bin Laden himself concluded, without Iran’s key support for al-Qaeda in the years following the 9/11 attacks, al-Qaeda would have collapsed, and al-Qaeda’s subsequent terrorist schemes carried out in Iraq through al-Qaeda-in-Iraq would not have come to fruition.

323. Iran’s strategy recognized that the Iranians could use their sectarian enemies, including Shia-haters like Zarqawi, to harm Iran’s two primary enemies, the United States and Israel, and pragmatically and ruthlessly to pursue Iranian interests throughout the world.

324. Iran and Soleimani pursued this strategy towards Sunni terrorists targeting Americans in Iraq at all relevant times because it inflicted harm on America while providing Iran

¹²⁴ *Id.*

¹²⁵ David Blair, *The Rise of the Fanatics that Now Control ISIL*, Sunday Independent (Apr. 12, 2015), 2015 WLNR 10684439.

iron-clad protection from being attacked by these same Sunni terrorists. Indeed, in a May 2014 message to Ayman al-Zawahiri from Abu Muhammad al-Adnani – who was once a Zarqawi ally and former al-Qaeda member but had departed with ISIS becoming its spokesman after ISIS and al-Qaeda split earlier in 2014 – Adnani reminded al-Qaeda, on behalf of ISIS, that:

ISIS has not attacked the Rawafid [Shia] in Iran since its establishment. ... It has kept its anger all these years and endured accusations of collaboration with its worst enemy, Iran, for refraining from targeting it, leaving the Rawafid [Shia] there to live in safety, acting upon the orders of al Qaeda to safeguard its interests and supply lines in Iran. Let history record that Iran owes al Qaeda invaluablely.

325. The four intelligence services that knew Zarqawi the best (other than Iran) – those of the U.S., Iraq, Jordan, and Germany – all concluded that Iran deliberately helped stand up Zarqawi’s terrorist network in Iraq. Like their U.S. and Iraqi counterparts, the Jordanian and German intelligence and law enforcement communities developed overwhelming evidence as to the sustained and substantial nature of Iran’s provision of material support and resources to Zarqawi.

326. Given Zarqawi’s Jordanian roots, Jordan’s intelligence service, the *Mukhabarat*, knew him as well as anyone. Jordanian intelligence concluded that Iran deliberately stood-up Zarqawi’s terrorist network in Iraq in order to inflict pain on Americans there and advance Iranian interests in the country, providing terrorist seed capital in the form of arms and early essential logistical support, and sustained Zarqawi’s network thereafter by permitting them to travel freely between Iran and Iraq as long as they continued attacking Americans in Iraq.

327. German intelligence and law enforcement also confirmed the close nexus between Zarqawi and Iran. In 2002, the German intelligence services, the *Bundesnachrichtendienst* (“BND”), successfully wiretapped and surveilled several members of the Zarqawi network in Germany, which allowed BND agents to precisely track Zarqawi’s travel patterns during and after

his flight from Afghanistan. Based on insights from these leads, German intelligence concluded that Zarqawi received refuge and medical care in Mashhad, Iran on January 5, 2002, and remained in Iran until at least April of 2002, during which time he directed the retreat of his al-Qaeda operatives from Afghanistan, through Iran, into to the Kurdistan region on both sides of the Iran/Iraq border. Thereafter, Zarqawi traveled to Tehran and Zahedan in support of his efforts to stand up al-Qaeda-in-Iraq. During this entire time, Zarqawi benefited from Iranian patronage and protection, including his own personal team of IRGC minders provided by Soleimani himself.

328. German law enforcement also developed solid evidence that Iran had provided essential material support to Zarqawi. According to files from Germany's Federal Office of Criminal Investigation, German prosecutors concluded that Iran gave Zarqawi essential state-sponsored terrorist support and was a key logistical partner for his terrorist enterprise in Iraq.

329. Other European counter-terror authorities concurred with the findings of U.S., Iraqi, Jordanian, and German governments. For example, a noted Spanish terrorism judge, Baltasar Garzon, concluded that al-Qaeda's board of managers were operationally active from their Iranian safe-haven, coordinating operations against America and its Coalition partners. Similarly, in 2004, French intelligence officials concluded that al-Qaeda leaders had permission to move within Iran and support terrorist operations against America from their Iranian safe-haven.

330. Iran – and Soleimani himself – recognized that Iran's support for Zarqawi advanced Iranian interests even after Zarqawi began slaughtering Shiites in Iraq. For example, Soleimani reportedly told the audience at an Iranian military seminar that the Qods Force permitted Zarqawi and more than a dozen of his senior terrorist followers to enter Iran whenever they pleased via border crossings between Ham and Halabja. At this same discussion, when asked why Iran supported Zarqawi given his anti-Shiite attacks, Soleimani reportedly replied that Zarqawi's

attacks in Iraq “serve the supreme interests of Iran” by stopping the formation of pro-American government in Iraq.

331. Even when al-Qaeda-in-Iraq began massacring Iraqi Shiites at scale in 2006, Iranian support for al-Qaeda-in-Iraq still advanced Iran’s perceived self-interest in Iraq by fostering anti-American violence there and by forcing Iraqi Shiites to seek protection from Iranian Shiite terrorist proxies, like Jaysh al-Mahdi, who were also fighting al-Qaeda-in-Iraq. As Mr. Sadjadpour explained, Zarqawi’s attacks against Shiites “totally radicalized the Shiite community in Iraq” and “essentially pushed them into the arms of Iran and Qassem Soleimani, who said to the Shiites of Iraq, we can protect you.”¹²⁶ Simply put, “[i]t served the interests of the Islamic Republic to maintain Iraq in a state of controlled chaos and anarchy.”¹²⁷

332. By supporting al-Qaeda-in-Iraq, Iran provided material support and resources for the extrajudicial killings that killed or injured Plaintiffs or members of their families. Al-Qaeda-in-Iraq directly participated in many of the attacks that killed or injured Plaintiffs or their family members. Moreover, al-Qaeda-in-Iraq was closely intertwined with al-Qaeda and Ansar al-Islam and associated terrorist groups acting in Iraq, and al-Qaeda-in-Iraq planned and authorized the Sunni attacks in which it did not directly participate. Material support and resources provided to al-Qaeda-in-Iraq thus also flowed to al-Qaeda and Ansar al-Islam, causing the injury and deaths of Plaintiffs or their family members.

iv. Iran Used the IRGC to Establish Ansar Al-Islam as an Iranian Sunni Terrorist Proxy in Iraq

333. To ensure Iranian influence in Kurdish communities on both sides of the Iran/Iraq border, and consistent with Iranian policy supporting anti-American terror in countries bordering

¹²⁶ Sadjadpour, *quoted in* NPR, *Throughline*.

¹²⁷ NPR, *Throughline*.

Iran, Ansar al-Islam has been, and remains to this day, a longstanding terrorist proxy of the IRGC. Iran, through the activities orchestrated by Qassem Soleimani and those acting at his instruction, was the proximate and but-for cause of Ansar al-Islam's existence and ability to commit attacks targeting Americans in Iraq, including against Plaintiffs.

334. Iran's support for Ansar al-Islam is rooted in the former's obsession over Kurdish issues and support for Sunni terrorists in Kurdistan was a foundation of Iranian efforts to exercise influence in Northern Iraq. This region had historically been beyond Baathist reach when Saddam ran Iraq, and it could provide an unbroken Iranian corridor across the "Shiite Crescent," which stretches from Iran through Iraq to Syria and Lebanon.

335. Ansar al-Islam could not exist, let alone pose a terrorist threat to Americans in Iraq, without the key assistance provided by Iran through the IRGC and Qods Force. As the anti-terrorism think tank, the Jamestown Foundation, concluded, "a significant degree of Iranian support was necessary for Ansar al-Islam to function, given that the group's military supplies came in from Iran (the mountainous region they controlled touches the Iranian border), veterans from Afghanistan joined them via Iran, and their cadres (including Mullah Krekar himself) entered and left the area via Iran."¹²⁸ Similarly, the International Crisis Group concluded that it was "indisputable ... that [Ansar al-Islam] could not survive without the support of powerful factions in neighbouring Iran, its sole lifeline to the outside world."¹²⁹

336. Contemporaneous American and British intelligence reports concerning Iran and Iraq support these conclusions.

¹²⁸ David Romano, *An Outline of Kurdish Islamist Groups in Iraq* at 12, The Jamestown Foundation (Sept. 2007) ("Romano, *An Outline of Kurdish Islamist Groups in Iraq*").

¹²⁹ International Crisis Group, *Radical Islam In Iraqi Kurdistan: The Mouse That Roared?* at 1-2, IRAQ Briefing (Feb. 7, 2003).

337. Al-Qaeda was responsible for the success of Ansar al-Islam's suicide bomb attacks against Americans in Iraq. Through its relationship with al-Qaeda and Ansar al-Islam, Iran was the proximate and but-for cause of Ansar al-Islam's suicide bombing attacks against Americans in Iraq.

338. Iran's support for al-Qaeda, al-Qaeda-in-Iraq, and Ansar al-Islam was mutually reinforcing. Zarqawi's ability to leverage safe havens on Iranian soil and his membership and leadership role in all three groups played a key role in facilitating AQI's development. By providing leadership, training, logistical support, and instruction to al-Qaeda, AQI, and Ansar al-Islam, Zarqawi created a network of al-Qaeda affiliated terrorists working together in a shared campaign against Americans in Iraq, which he then leveraged to attack Americans throughout Iraq.

339. By supporting Ansar al-Islam, Iran provided material support and resources for the extrajudicial killings that killed or injured Plaintiffs or members of their families. Ansar al-Islam directly participated in some of the attacks that killed or injured Plaintiffs or their family members. Moreover, Ansar al-Islam was closely intertwined with al-Qaeda, al-Qaeda-in-Iraq, and associated terrorist groups acting in Iraq, and Ansar al-Islam provided essential logistical support for the entire Sunni campaign by facilitating the smuggling of weapons into Iraq, and therefore Ansar al-Islam aided the Sunni attacks in which it did not directly participate. Material support and resources from Iran provided to Ansar al-Islam thus also flowed to al-Qaeda and al-Qaeda-in-Iraq, causing the injury and deaths of Plaintiffs or their family members.

340. Consistent with Iran's policy of material support to al-Qaeda, al-Qaeda-in-Iraq, and Ansar al-Islam (collectively, Iran's "Sunni Terrorist Proxies") described above, Iran provided material support or resources to al-Qaeda, al-Qaeda-in-Iraq, and Ansar al-Islam for the acts of extrajudicial killing that killed or injured Plaintiffs or their family members. As explained below,

that support took the form of “currency . . . lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, . . . and transportation.”¹³⁰

v. Iran Provided its Iraqi Sunni Terrorist Proxies with Weapons, Explosives, and Lethal Substances

341. Iran provided material support or resources for the acts of extrajudicial killing that killed or injured Plaintiffs, or their family members, by providing (among other things) weapons, explosives, and lethal substances to the al-Qaeda, al-Qaeda-in-Iraq, and Ansar al-Islam.

342. Iran provided a regular flow of weapons and military equipment to Sunni terrorists targeting Americans in Iraq, including al-Qaeda, al-Qaeda-in-Iraq, and Ansar al-Islam. According to a senior al-Qaeda terrorist, “the Quds Force . . . supplied Zarqawi with weapons” and as a result, the al-Qaeda member concluded that, if “Osama was responsible for financing the butchers of Baghdad [i.e., Zarqawi and al-Qaeda-in-Iraq], so was Tehran.”

343. Middle Eastern and Western intelligence services concurred with this assessment and have long documented Iran’s provision of weapons and equipment to Sunni terrorists targeting Americans. As one Jordanian intelligence professional explained, placing himself from the perspective of a Sunni extremist (paraphrased) “I go to the Saudis when I need money and I go to the Iranians when I need arms, training, or supplies.”

344. Regional Kurdish security officials also documented Iran’s provision of weapons and equipment to Sunni terrorists targeting Americans in Iraq. “[I]n the town of Tuwella, the local PUK [Patriotic Union of Kurdistan, a large political party] chief, Ismail Ameen, said [that] . . . [j]ust before the war, in February 2003, he saw six gray Toyota Landcruisers drive into town from the

¹³⁰ 18 U.S.C. § 2339A(b)(1).

Iranian border. He said the trucks were loaded with bullets and mortar shells for [an al-Qaeda affiliate's] fighters. 'They would have run out of ammunition . . . without the supplies they got from Iran,' he said. Two top PUK security officials, and three members of the PUK's political bureau, also contended that Iran has continued to support Islamist insurgents."¹³¹ As one report explained in 2004:

For years, and with the blessing of Iranian officials, Islamist terrorist groups have smuggled weapons ... into Iraq ... many Kurdish intelligence and security officials said. ... [H]ere in the mountains of Kurdistan ... are tangible footprints of Iran's collaboration with terror and insurgent groups responsible for attacks inside Iraq. According to a half-dozen officials in the Patriotic Union of Kurdistan,... Iran has extended its network of agents inside Iraq. Iran, the officials say, continues to aid groups like Ansar al-Islam and Abu Musab al-Zarqawi's group, now named Al Qaeda in Mesopotamia. Even though Iran is a Shi'ite theocracy, these officials said, it helps Sunni insurgent groups because it wants to prevent a strong unified government from taking shape in Iraq. "They go back and forth after running missions here," said Anwar Haji Othman, head of security in the area ... including a long stretch of the Iranian border.¹³²

345. Regional papers in the Middle East also agree with this conclusion. As one Bahraini paper observed, Iran's decision to "transfer[] munitions to Sunni extremists fighting the Americans in Iraq," accords with similar decisions Iran made to "export[] weapons to the Taliban" and other anti-American terrorists who did not follow the Khomeneist school of Iranian theological supremacy like "the Zaidi Houthis" and "Syria's Alawites ... [who] hail from significantly different schools of Islam."¹³³

346. Iran also funneled weapons to Sunni terrorists in Iraq through its proxy, Ansar al-Islam. Given its location on both sides of the Iran/Iraq border, Ansar al-Islam could not have

¹³¹ Thanassis Cambanis, *Along Border, Kurds Say, Iran Gives Boost To Uprising*, Boston Globe (Nov. 7, 2004), 2004 WLNR 6887856 ("Cambanis, *Along Border*").

¹³² *Id.*

¹³³ DT News (Bahrain), *Why is Tehran Recruiting Daesh Jihadists?* (Nov. 5, 2018), 2018 WLNR 34281745

sourced any of its supplies or fighters without the active cooperation of the IRGC and the Qods Force. As the Jamestown Foundation concluded, Ansar al-Islam's "military supplies came in from Iran," as did the group's fighters, who had depended upon the cooperation of Iran to transit through Iran (between Iraq and the Afghanistan-based camps they also attended) as well as to provide a safe-haven from which to plan attacks.¹³⁴

347. After American forces destroyed Ansar al-Islam's camp in Iraqi Kurdistan in March 2003, Zarqawi and his Ansar al-Islam lieutenants fled to Iran, where they regrouped, rearmed, trained, and continued to plan operations against Americans in Iraq, all while "Iran continued to supply Ansar al-Islam and its ally, Abu Musab al-Zarqawi, smuggling supplies for the insurgency against the U.S. and its coalition partners. In this way, the Zarqawi-Iran connection was maintained from his retreat from Afghanistan to his arrival in Iraq."¹³⁵

348. Indeed, as the *Boston Globe* reported in 2004, "[f]or years, and with the blessing of Iranian officials," Ansar al-Islam "smuggled weapons ... into Iraq on this [Iranian] road [near the Iraqi border], many Kurdish intelligence and security officials said."¹³⁶

349. Ansar al-Islam received weapons and munitions from Iran, including Katyusha rocket launchers, mortar rounds, and the ubiquitous Toyota Land Cruiser SUVs used by Ansar al-Islam, which "could not have been smuggled into the area without the tacit approval of the Iranian government and security apparatus."¹³⁷

¹³⁴ Romano, *An Outline of Kurdish Islamist Groups in Iraq*.

¹³⁵ Dore Gold and Lt. Col. (Res.) Jonathan D. Halevi (Israel Defense Forces), *Zarqawi and Israel: Is There a New Jihadi Threat Destabilizing the Eastern Front?*, Jerusalem Center for Public Affairs, Jerusalem Issue Brief Vol. 5 No. 12 (Dec. 15, 2005) ("Gold and Halevi, *Zarqawi*").

¹³⁶ Cambanis, *Along Border*.

¹³⁷ The Washington Institute for Near East Policy, *The Islamist Threat from Iraqi Kurdistan* (Dec. 1, 2001).

350. Iranian support was also key to al-Qaeda's and its affiliates' ability to execute their signature attacks. Al-Qaeda's IEDs and suicide bomb attacks offer two examples. With respect to the former, Iranian aid was key to the success of Sunni terrorists' campaign of IED attacks against Americans in Iraq. Coalition personnel on the ground in Iraq concluded that Iran provided substantial IED-related support to Sunni terrorists targeting Americans in Iraq. For example, by the summer of 2006, Task Force 16 members responsible for hunting al-Qaeda-in-Iraq terrorists had concluded that Iran was providing sophisticated IED technology to Sunni terrorists in Iraq, led by al-Qaeda, in order to inflict casualties on Americans in Iraq. British military personnel in Iraq reached a similar conclusion a year prior when, in 2005, "a senior British general repeated a claim that bomb-making technology is crossing into Iraq from Iran."¹³⁸ As reported at the time:

Major-General Jim Dutton, who commands a multinational force in south-eastern Iraq, said the know-how for advanced bombs was coming 'across that border'. ... Defence sources quoted independently by the BBC were more blunt, saying that the Revolutionary Guards, an elite fighting force appointed by the country's supreme leader, were indeed giving original bomb-making training to Iraq's insurgents. At first and even second glance, allegations of an alliance between Iran and Al-Qaeda, especially if it incorporates cells affiliated to the terror organisation presently operating in Iraq, defies all sense and logic. For a start, Iran is Persian/Shi'ite, while Al-Qaeda is Arab/Sunni. ... [I]t now seems clear that Iran and Al-Qaeda generally have been drawn together, despite their obvious ideological and religious differences, by a common goal: To facilitate global jihad and help hasten American failure in Iraq.¹³⁹

351. Iran also helped provide al-Qaeda, al-Qaeda-in-Iraq, and Ansar al-Islam the "weapons" they used when they deployed suicide bombers in Iraq, as Iran was the original source of the groups' collective embrace of suicide bombing as a tactic, and Iranian geography was

¹³⁸ John R. Bradley, *Real Threat From Iran Is Here, Now*, Straits Times (Singapore) (Nov. 14, 2005), 2005 WLNR 18356274 ("Bradley, *Real Threat From Iran*").

¹³⁹ Bradley, *Real Threat From Iran*.

necessary for the travel of suicide bombers into Iraq, which in the case of a suicide bomber accomplished the “insertion” of the weapon into the country.

352. Separately, Iranian territorial aid was also key to the success of al-Qaeda’s IED attacks and suicide bombs because only through Iran could al-Qaeda and its affiliates maintain the CAN fertilizer supply chain from the Pakistani supplier upon which they relied. As a result, al-Qaeda could not have executed its campaign of fertilizer-based suicide bomb and IED attacks against Americans in Iraq without the terrorist land bridge provided by Iran. On information and belief, al-Qaeda sourced some of its fertilizer for use in their Iraqi bombs from a supplier in Pakistan and transported such fertilizer across from Pakistan to Iraq by using the terrorist land bridge offered by Iran, which al-Qaeda could not have accomplished without the aid of the IRGC, which controls Iran’s borders with Afghanistan and Iraq, and whose permission is necessary to transport any goods overland from the above-described route from Pakistan to Iraq.

vi. Iran Provided its Iraqi Sunni Terrorist Proxies with Lodging, Training, Expert Advice or Assistance, Safehouses, Personnel, and Transportation

353. Iran also provided its Sunni Terrorist Proxies in Iraq with lodging, training, expert advice or assistance, safehouses, and transportation. Iran taught its Sunni Terrorist Proxies attack techniques that were particularly effective against U.S. and Coalition forces. Without the training, lodging, safehouses, and transportation assistance from Iran and its agents, Iran’s Sunni Terrorist Proxies would not have been able to launch as successful a terrorist campaign against Americans in Iraq.

354. **Lodging, Safehouses, and Transportation.** Iran has maintained a decades-long travel assistance relationship with al-Qaeda as part of the terrorist alliance between Iran, al-Qaeda, and Lebanese Hezbollah.

355. By no later than January 2002, the Qods Force had approved a strategic plan to actively support al-Qaeda's post-9/11 terrorist attacks against Americans in the Middle East by providing sanctuary in Iran to senior al-Qaeda terrorists and their family members, directly supported and managed by the Qods Force. To facilitate al-Qaeda members' flight from Afghanistan to their newfound Iranian safe-haven, the Qods Force relied upon the assistance of Zarqawi – whom it already knew based on his travels in the region – to coordinate the travel of senior Qaeda operatives, including Saif al-Adel, from Afghanistan to Iran.

356. Sitting between Iraq and Afghanistan and having a long history of facilitating Sunni terrorist travel and logistics, Iran was ideally suited to aid the ascendant Sunni insurgency in Iraq after March 2003 because al-Qaeda's assistance could only flow from Afghanistan to Iraq via Iran. Reporting the views of Kurdish security officials, one journalist explained in 2004 that there is a long history in the Middle East “of nations giving shelter to their enemies’ enemies” and thus “[t]he apparent Iranian ties to [Sunni] mujahedeen groups operating inside Iraq only continue[d] this long Machiavellian tradition,” and reflected Iran's willingness to “work with [Sunni] groups ... whose ideology is so opposed to theirs, because they want to have a card to play in Iraq.”¹⁴⁰

357. Iran's service as the “terrorist land bridge” by its provision of travel assistance to al-Qaeda and al-Qaeda-in-Iraq was essential to the terrorists' ability to conduct attacks against Americans in Iraq. As Judge Daniels found in another case against Iran,

Perhaps the most important form of aid Iran gave al Qaeda prior to 9/11 (and continues to give today) involves the facilitation of travel. ... Travel assistance “is invaluable,” not only to avoid detection and arrest, but established lines of transit make recruitment and training easier, as individuals can travel to and from training camps without fear of interference. Also, travel facilitation enables better communication and coordination. Even before 9/11, al Qaeda was aware that the United States monitored phones and other forms of communication and recognized

¹⁴⁰ Cambanis, *Along Border*.

that many sensitive deliberations are best done face-to-face. Doing so requires individuals who can travel freely from one area to another.¹⁴¹

358. “In the mid–1990s, when the Iran–Hizballah–al Qaeda terror alliance was forming, al Qaeda operative Mustafa Hamid had ‘negotiated a secret relationship with Iran that allowed safe transit via Iran to Afghanistan.’”¹⁴²

359. “Numerous admissions from lower level al Qaeda members who were interrogated at the detention facility at Guantanamo Bay confirm the existence of the clandestine Iran–Afghanistan passageway, managed by MOIS. Al Qaeda had ‘total collaboration with the Iranians,’ and had its own organization in Iran ‘that takes care of helping the mujahedin brothers cross the border.’”¹⁴³ “By ... providing safe passage through Iran and into Afghanistan, and by permitting Hezbollah to receive the traveling group ... Iran, in essence, acted as a state sponsor of terrorist travel.”¹⁴⁴ These trends have continued without interruption since the 1990s.

360. After 9/11, Iran provided safehouses to many senior leaders of al-Qaeda and their families, including Osama bin Laden’s sons. Iran permitted these senior leaders to move freely within Iran in the early 2000s, while they continued to direct, organize, and support al-Qaeda’s terrorist operations throughout the world.¹⁴⁵ In essence, Iran provided al-Qaeda with a safe haven from which to orchestrate its terrorist activities.¹⁴⁶ As Judge Daniels found:

When the United States-led multi-national coalition attacked the Taliban regime in Afghanistan in the fall of 2001, Iran facilitated the exit from Afghanistan, into Iran, of numerous al Qaeda leaders, operatives, and their families. The Iran–Afghanistan

¹⁴¹ *In re Terrorist Attacks on Sept. 11, 2001*, 2011 WL 13244047, at *28 (findings of fact).

¹⁴² *Id.* at *17 (findings of fact) (internal citations omitted).

¹⁴³ *Id.* (internal citations omitted).

¹⁴⁴ *Id.* (internal citations omitted).

¹⁴⁵ *Id.*

¹⁴⁶ *Id.* at 150-51 (“When a foreign sovereign allows a terrorist organization to operate from its territory, this meets the statutory definition of ‘safehouse.’”).

safe passageway, established earlier to get al Qaeda recruits into and out of the training camps in Afghanistan, was utilized to evacuate hundreds of al Qaeda fighters and their families from Afghanistan into Iran for safe haven there. The IRGC knew of, and facilitated, the border crossings of these al Qaeda fighters and their families entering Iran.

Osama bin Laden's friend, Gulbuddin Hekmatyar, who was then in exile in Iran near the Afghan border, was instrumental in the evacuation of al Qaeda into Iran, as were Imad Mughniyah and Iran's Qods Force commander Ahmad Vahidi.

Among the high-level al Qaeda officials who arrived in Iran from Afghanistan at this time were Saad bin Laden and the man who would soon lead "al Qaeda in Iraq," Abu Mussab Zarqawi.¹⁴⁷

361. The Coalition's civilian military leadership in the United States and Iraq also concluded that Iran provided such safe haven support to Zarqawi and other AQI terrorists.

362. The list of al-Qaeda-affiliated terrorists who supported al-Qaeda attacks against Americans from their post 9/11 Iranian safe-haven reads like an al-Qaeda management roster, featuring nearly two dozen senior leaders, organizers, planners, ideologues, and terrorist operatives from around the world – comprising most of al-Qaeda's military council between from 9/11 through 2015. The following terrorists all sheltered at the Qods Force facility in Tehran, and most (all but Zarqawi, who died a year earlier) were witnessed by a person who visited the facility on or about 2007:

- **Osama bin Laden's family**, including sons Saad, Mohammad, Othman, Ladin, and Hamza (one of whom even got married in Iran), wife Najwa, and daughter Iman;
- **Abu Musab al-Zarqawi**, who launched al-Qaeda-in-Iraq's campaign against America from Iran;
- **Abu Muhammad al-Masri**, al-Qaeda's chief of foreign relations and a senior member of al-Qaeda's military council who became al-Qaeda's the number 2 overall, behind only Zawahiri, after bin Laden was killed in 2011, and who managed al-Qaeda operations from his safe haven in Iran from 9/11 until he was killed in Tehran by Mossad agents on August 7, 2020;

¹⁴⁷ *Id.* at *25 (internal citations omitted).

- **Saif al-Adel**, al-Qaeda's military chief and number 3 overall, who, among other things, personally managed al-Qaeda's support for Zarqawi and the Zarqawi/bin Laden relationship, was tasked with facilitating al-Qaeda's support for the Sunni insurgency against Americans in Iraq from Iran, and directed anti-American attacks from Iran under the wing of the Qods Force;
- **Abu Musab al-Suri**, a senior al-Qaeda strategist who was one of the most important thinkers for the group;
- **Mahfouz Ibn El Waleed**, a key member of al-Qaeda's leadership council and its sharia committee, who helped approve and justify attacks against America from his safe haven in Iran;
- **Abu Dagana al-Alemani**, a senior al-Qaeda attack planner who coordinated al-Qaeda's logistical support for its global affiliates from Iran; and
- **Sulaiman Abu Ghaith**, who served as al-Qaeda's spokesman from Iran and helped rally support for al-Qaeda's anti-American jihad from there.

363. Among the senior al-Qaeda leaders who fled to Iran after 9/11, most remained ensconced in Iran thereafter, never leaving their Iranian safe-haven while continuing to support the jihad against America. Zarqawi and his lieutenants were the one notable exception: they accepted the Qods Force's offer of money, arms, and transportation from Kurdistan to Baghdad, all of which they used to launch their terror campaign against Americans in Iraq and launch al-Qaeda-in-Iraq's campaign against Americans there.

364. Iran's safe haven support for al-Qaeda did not diminish in the years after 9/11. For example, in 2011, Judge Daniels found, as a matter of law, that "[s]ince the 9/11 attacks, and continuing to the present day, Iran continues to provide material support and resources to al Qaeda in the form of safe haven for al Qaeda leadership and rank-and-file al Qaeda members."¹⁴⁸

365. As the *Washington Post* reported after al-Qaeda's number 2, Masri, was killed in Tehran in 2020, "[m]any of al-Qaeda's senior commanders have been sheltered in Iran, though one

¹⁴⁸ *In re Terrorist Attacks on Sept. 11, 2001*, 2011 WL 13244047, at *41 (findings of fact).

by one, they have been killed in recent years. With Masri's death, the only remaining member of al-Qaeda's shura council — its core leadership — with operational al-Qaeda terrorist experience is Saif al-Adel, who is believed still to be in Iran.”¹⁴⁹

366. Iran’s assistance also extended to permitting al-Qaeda and its affiliates, like al-Qaeda-in-Iraq, to use Iran as a safe-haven from which to plan and prepare attacks against Americans in Iraq. As Judge Daniels found, after 9/11, “[t]here have been numerous instances of al Qaeda operatives and leaders meeting, planning, and directing international terrorist operations from the safety of Iranian territory. Senior al Qaeda members continued to conduct terrorist operations from inside Iran.”¹⁵⁰

367. In August 2003, Iran facilitated a meeting in Tehran between lieutenants from al-Qaeda-in-Iraq and Ansar al-Islam, in which the participants agreed in Zarqawi’s name to establish a permanent terrorist base in Kurdistan to facilitate attacks against Americans and ensure the smooth functioning of the pipeline between the Arab world and Afghanistan, which ran through Iran and was essential to Sunni terrorists supply of weapons, funds, and personnel.

368. In Tehran, the Qods Force operated a facility for al-Qaeda and al-Qaeda-in-Iraq leaders and operatives that was known as “Block 300.” At Block 300, the Qods Force provided shelter, communications, training, and other assistance to al-Qaeda and al-Qaeda-in-Iraq terrorists from 2001 through the present day. For example, in August 2007, a visitor to Block 300 saw bin Laden’s sons Saad, Mohammed, Othman, Hamzah, and Ladin, as well as Saif al-Adel, Abu al-Khayr al-Masri, and Sulaiman Abu Ghaith. The same visitor in 2007 observed that all of al-

¹⁴⁹ Ellen Nakashima, *Israel, At Behest of U.S., Killed al-Qaeda’s Deputy in a Drive-By Attack in Iran*, Washington Post (Nov. 14, 2020), 2020 WLNR 32556539

¹⁵⁰ *In re Terrorist Attacks on Sept. 11, 2001*, 2011 WL 13244047, at *25 (findings of fact) (internal citations omitted).

Qaeda's military council was present at Block 300 other than Zawahiri and Sheikh Saeed al-Masri. Key female members of bin Laden's family were also housed at Block 300.

369. Soleimani personally assigned two senior Qods Force officers to see to the needs of the senior al-Qaeda leaders and their family members sheltering at Block 300. Throughout, the Qods Force provided senior al-Qaeda leaders with everything they needed to sustain their leadership inside Iran and maintain the morale of their military council and their families, including generous residential accommodations, trips to luxury shopping destinations, gym memberships, and the finest medical care in Iran (which was otherwise only available to the clerics and senior leaders of the Iranian regime).

370. Al-Qaeda's relationship with its Qods Force protectors was so warm that al-Qaeda's military council and bin Laden's sons invited their Qods Force handlers to break their Ramadan fast with them at Block 300. The Qods Force responded by taking al-Qaeda's military council out to a five-star restaurant for an *iftar* meal. Days later, Soleimani himself arrived in person at Block 300 to celebrate Eid with bin Laden's sons, joining them to break the fast.

371. At this time, al-Qaeda depended upon the assistance of the Qods Force to maintain al-Qaeda's Iran pipeline, through which the group moved funds and personnel between the Middle East and its home base in Pakistan.

372. In meetings at Block 300 on or about 2007 and 2008, Iranian officials met with the designated leader of the al-Qaeda and al-Qaeda-in-Iraq terrorists who were sheltering in their Qods Force-provided safe-haven. During these meetings, the Iranian officials told al-Qaeda and al-Qaeda-in-Iraq, through their designated spokesman at Block 300, in sum and substance, that the welfare of bin Laden's family was Soleimani's personal responsibility. By this time, Soleimani had a positive relationship with bin Laden's sons residing in Iran, who referred to Soleimani as

“Hajji Qassem” and relayed to other al-Qaeda leaders that Soleimani and al-Qaeda had both been targeted by America and should therefore work together. At these meetings, the Iranian officials and al-Qaeda agreed that they should cooperate regarding the conflict in Iraq.

373. In one meeting at Block 300 on or about 2008, Soleimani addressed al-Qaeda’s senior leaders, as well as bin Laden’s family, and stated that “I did my best to serve you” and “I stopped those who wanted to hurt you.” Soleimani also made it clear on multiple occasions to al-Qaeda’s leaders that Iran remained willing to continue helping as long as Iran benefited.

374. Soleimani continued to personally tend to his al-Qaeda assets at Block 300 until Soleimani’s own demise in 2020. For example, after bin Laden was killed in 2011, to try to break the malaise that had overtaken Block 300, Soleimani instructed his Qods Force deputies to take the al-Qaeda women and children on a trip for shopping and to an amusement park, while al-Qaeda’s assembled *shura* in Iran could discuss strategy.

375. In 2015, an intelligence review at the Defense Intelligence Agency confirmed additional measures of Iran’s support for al-Qaeda, including Iranian facilitation of al-Qaeda travel between Iraq and Pakistan.

376. Iran also provided transportation assistance, lodging and safe-haven assistance to al-Qaeda-in-Iraq terrorists, including Zarqawi himself and other senior leaders of the group. In doing so, Iran provided similar lodging, training, expert advice or assistance, safehouses, and transportation to al-Qaeda-in-Iraq as it did for al-Qaeda.

377. Zarqawi had deep relations in Iran owing to his status as the top terrorist and operator at al-Qaeda’s training camp in Herat, Afghanistan, close to the Iranian border.

378. After 9/11, Zarqawi took refuge in Iran and established new al-Qaeda training camps and safe houses inside Iran at sites in Zahedan, Isfahan, and Tehran. From his new Iranian

safe-haven, Zarqawi invited his followers, including seasoned terrorists in Europe, to travel to Tehran to meet with him, bringing money and receiving instructions from Zarqawi.

379. To facilitate al-Qaeda-in-Iraq's communications and attack planning, the Qods Force provided AQI with phone and facsimile numbers and facilitated AQI's use of couriers. With respect to the former, the Qods Force provided substantial communications support to al-Qaeda-in-Iraq, including the following numbers for AQI's use courtesy of Iran: 0X9X-9X1X3X1X3X, 0X9X-9X1X3X9X4X, 0X9X-2X8X5X6X8, and 0X9X-9X3X1X3X9X.¹⁵¹

380. During this time, the Qods Force also provided false documents to al-Qaeda-in-Iraq leaders and operatives to aid in their ability to move between Iran, Iraq, Afghanistan, Syria, Lebanon, and Jordan. For example, the Qods Force arranged for special passports and false documents for Zarqawi and his fighters to be able to enter Iraq without a visa.

381. Zarqawi's apparent close relationship with the Syrian regime – which is Iran's closest nation-state ally – corroborates the existence of his alliance with Iran. Given the Syrian regime's support for the Iraqi insurgency, the ease with which Zarqawi was able to enter and exit Syria, and the regular flow of some AQI recruits through Syria into western Iraq, it is reasonable to conclude that Zarqawi had a close and collaborative relationship with the Syrian regime. Given Syria's status as an Iranian client, such relations further corroborate Zarqawi's receipt of support from Iran, as Syria would not have supported such activities without Iran's blessing.

382. Iran also provided safe-haven to other senior AQI leaders in addition to Zarqawi. Based on the confession of one of Zarqawi's Jordanian associates, Ahmad Mahmud Salih Al-Riyati, who was detained by Coalition forces in March 2003, Jordanian intelligence confirmed that nearly all the senior leaders of Zarqawi's group had been sheltering and planning attacks from

¹⁵¹ Plaintiffs have redacted every other number in the numbers affiliated with Zarqawi.

Iran. Jordanian intelligence also concluded that Zarqawi himself probably directed al-Qaeda-in-Iraq's attacks against Americans in Iraq from his safe-haven in Iran.

383. **Training, Expert Advice or Assistance, and Personnel.** Iran's (including Lebanese Hezbollah's) training of the IRGC's Sunni Proxies in small unit tactics, small arms, explosives, indirect fire, and other techniques enabled the Sunni Proxies to more effectively attack Americans in Iraq. The Sunni Proxies in Iraq used Iran's training to kill or injure Plaintiffs or their family members.

384. Like its transportation assistance to al-Qaeda, Iran has also maintained a decades-long training relationship with al-Qaeda as part of the terrorist alliance between Iran, al-Qaeda, and Lebanese Hezbollah.

385. Iran, through the IRGC and Hezbollah, served as the original trainer for al-Qaeda with respect to suicide bombings, attacks against large buildings, IEDs, explosives, intelligence, and general tactics for attacks directed at American interests. For example, senior al-Qaeda operatives traveled to Iran and Lebanon during this period to camps run by Hezbollah and sponsored by the Qods Force.¹⁵² The operatives received advanced explosives training that enabled al-Qaeda to launch large-scale terrorist attacks on American embassies in Africa.¹⁵³ According to one senior al-Qaeda official, trainers at this time were already researching how to develop shaped charges to pierce armor plating – the technology later perfected in Iranian EFPs.

386. As Judge Daniels found in another case against Iran, "[t]hroughout the 1990s, the al Qaeda–Iran–Hizballah terrorist training arrangement continued. Imad Mughniyah himself

¹⁵² *Owens v. Republic of Sudan*, 826 F. Supp. 2d 128, 151 (D.D.C. 2011) ("Prior to al Qaeda members' training in Iran and Lebanon, al Qaeda had not carried out any successful large scale bombings.").

¹⁵³ *Id.*

coordinated these training activities, including training of al Qaeda personnel, with Iranian government officials in Iran and with IRGC officers working undercover at the Iranian embassy in Beirut, Lebanon. At all times, Iran's Supreme Leader was fully aware that Hizballah was training such foreign terrorists."¹⁵⁴

387. Through its relationship with al-Qaeda and al-Qaeda-in-Iraq, Iran was the proximate and but-for cause of al-Qaeda-in-Iraq's suicide bombing attacks against Americans in Iraq, because Al-Qaeda was responsible for the success of al-Qaeda-in-Iraq's suicide bomb attacks against Americans in Iraq, and al-Qaeda itself could not have survived after 9/11 without the key support provided by Iran.

388. Iran also provided training to Zarqawi and other al-Qaeda-in-Iraq terrorists at IRGC training camps in Iran. Indeed, on or about 2004, Soleimani reportedly boasted that Zarqawi had trained at an IRGC camp in Mehran, Iran, and that Zarqawi and his network were free to travel between Iran and Iraq through multiple IRGC-controlled border crossings.

389. Iraqi officials also confirmed Iran's key logistical support for Zarqawi's terrorist campaign in Iraq. For example, in December 2004, a senior Iraqi defense official publicly alleged – based on information derived from an interrogation of an al-Qaeda-in-Iraq operative who had been detained in Iraq – that Iran and Zarqawi were working together to train AQI terrorists at IRGC facilities in Iran.

390. By 2004, Iran's relationship with Zarqawi grew to be so open and notorious that the "United States ... warned Iran against providing any type of support to Al-Qaeda-linked

¹⁵⁴ *In re Terrorist Attacks on Sept. 11, 2001*, 2011 WL 13244047, at *12.

foreign militant Abu Mussab al-Zarqawi and his Tawhid wal Jihad (Unity and Holy War) group, saying such backing would be a ‘very, very serious matter.’”¹⁵⁵

391. As Judge Daniels found, “[t]he IRGC maintained a separate terrorist training camp especially for Saudi nationals because of their distinct cultural habits and religious practices. This training camp was located in Iraqi Kurdistan and controlled first by Iranian intelligence and later by Abu Musab Zarqawi, later to be the notorious head of ‘al Qaeda in Iraq.’”¹⁵⁶

392. Iran’s provision of lodging, safe harbor, and transportation to key al-Qaeda-in-Iraq leaders, including but not limited to, Zarqawi, was the but for and proximate cause of the formation of al-Qaeda-in-Iraq in the first instance.

393. Iran also provided logistical, training, and safe-haven directly to Ansar al-Islam terrorists targeting Americans in Iraq. As documented in a U.S. intelligence report, “there were approximately 320 Ansar al-Islam terrorists being trained in Iran . . . for various attack scenarios including suicide bombings, assassinations, and general subversion against U.S. forces in Iraq.” Similarly, a British defense report noted “some elements [of Ansar al-Islam] remain in Iran. Intelligence indicates that elements [of Iran’s Islamic Revolutionary Guard Corps] are providing safe haven and basic training to Iran-based [Ansar al-Islam] cadres.”

vii. Iran Provided its Iraqi Sunni Terrorist Proxies with Financial Support

394. Iran also provided financial support to al-Qaeda, al-Qaeda-in-Iraq, and Ansar al-Islam for the purpose of causing violence against Americans in Iraq. Iran accomplished this financial support through a number of direct and indirect means.

¹⁵⁵ Agence France-Presse English Wire, *US Warns Iran Against Any Support For Zarqawi* (October 18, 2004).

¹⁵⁶ *In re Terrorist Attacks on Sept. 11, 2001*, 2011 WL 13244047, at *12.

395. In some instances, Iran directly paid money to Sunni terrorists. For example, regional Kurdish security officials documented Iran's provision of cash to Sunni terrorists cycling back and forth between Iraq and their safe havens in Iran:

For years, and with the blessing of Iranian officials, Islamist terrorist groups have smuggled ... money into Iraq ... When US special forces and Kurdish peshmerga fighters attacked Ansar al-Islam, an Al Qaeda affiliate, in March 2003, hundreds of its members fled to Iran, the officials said, and have regrouped in several towns just over this border. There, they continue to ... raise funds, and plan terrorist operations in Iraq ... Iraqi and US officials have grumbled for more than a year about what they perceive as Iranian interference in Iraq. ... According to a half-dozen officials in the Patriotic Union of Kurdistan, known as the PUK, which controls the southern half of the Kurdistan region of Iraq, and commanders in the peshmerga, the force that provides security in the region, Iran has extended its network of agents inside Iraq. Iran, the officials say, continues to aid groups like Ansar al-Islam and Abu Musab al-Zarqawi's group, now named Al Qaeda in Mesopotamia. Even though Iran is a Shi'ite theocracy, these officials said, it helps Sunni insurgent groups because it wants to prevent a strong unified government from taking shape in Iraq. "They go back and forth after running missions here," said Anwar Haji Othman, head of security in the area around Halabja, including a long stretch of the Iranian border. "They bring cash from Iran to Iraq across the border."¹⁵⁷

396. When it imposed sanctions in 2011, the Obama Administration recognized the funding nexus between Iran and al-Qaeda. Moreover, "Obama Administration officials have stated that senior Iranian officials know about the money transfers and allow the movement of al-Qaeda foot soldiers through Iranian territory."¹⁵⁸

397. Iran specifically funded Zarqawi's terrorist campaign against Americans in Iraq. According to a senior al-Qaeda terrorist, "the Quds Force ... supplied Zarqawi with ... money. If Osama was responsible for financing the butchers of Baghdad [i.e., Zarqawi], so was Tehran."

398. As two terrorism scholars explained:

The critical point is that there is considerable evidence that Zarqawi may have developed an Iranian connection for financial and logistical support. It was not the

¹⁵⁷ Cambanis, *Along Border*.

¹⁵⁸ *In re Terrorist Attacks on Sept. 11, 2001*, 2011 WL 13244047, at *26.

first time Shiite Iran reached out to radical Sunni terrorist organizations. For years, Iran has sponsored Palestinian Islamist groups, particularly Islamic Jihad but also Hamas, as well. Iran had a constant interest to reach out beyond the Shiite Islamic communities of the Middle East to the much wider Sunni Muslim world, and Zarqawi had objective needs that could be met by Iran. Unlike Osama bin Laden, who could fall back on his own family's wealth and the backing of both Saudi charities and individuals, Zarqawi came from a poor background in Jordan. To wage his terrorist campaign, he needed state backing from somewhere. Indeed, *Al-Sharq al-Awsat* wrote in May 2004 that the Iranians had offered Zarqawi about \$900,000 and explosives. The same Arabic source reported in August that Brig.-Gen. Qassem Suleimani of the Revolutionary Guards was asked why Iran backs Zarqawi, given his attacks on Shiites. Suleimani reportedly answered that Zarqawi's actions serve the interests of Iran by undermining the emergence of a pro-U.S. government in Iraq.¹⁵⁹

399. Like its relationships with al-Qaeda and al-Qaeda-in-Iraq, Iran also provided substantial financial assistance to Ansar al-Islam terrorists to underwrite their attacks against Americans in Iraq.

400.

D. In Furtherance Of The Conspiracy, Hezbollah, The Qods Force, And Regular IRGC Operated As An Integrated Transnational Terrorist Organization With A Common Doctrine, Strategy, Financial Structure, Logistics Structure, And Command-And-Control

1. The IRGC's Transnational Terrorist Strategy, Doctrine, And Tactics Emphasize The Deployment Of Joint Cells Of Terrorists Led By Hezbollah, Funded And Resourced By The Qods Force, And Supported By Local Iranian Terrorist Proxies

401. Hezbollah, the Qods Force, and Regular IRGC, have long followed a common terrorist strategy and doctrine, which deploys common tactics across all three IRGC components – including the use of Hezbollah as the cell leader and Qods Force as cell funder and logistician – and every geography in which the IRGC or any of its proxies operate.

¹⁵⁹ Gold and Halevi, *Zarqawi*.

402. The IRGC adheres to an integrated global terror strategy, and follows the same rules for terrorist tradecraft, out of a recognition that it and its proxies were likely to always suffer from a resource deficit, making the intelligent deployment of its human assets paramount. Given these “equipment and logistical constraints, Hezbollah – with the guidance of Iranian advisors – adopted a doctrine of guerrilla warfare against the Israeli occupation.”¹⁶⁰

403. The Joint Cell approach is the foundation of the IRGC’s terrorist doctrine and the cornerstone of the Hezbollah Division’s entire terrorism “business model” when, as in most use cases, the Hezbollah Division and Qods Force are being deployed outside of Iran, or are being deployed inside of Iran but specifically to target Americans, e.g., to torture an American hostage being held in Iran, or to plan for a raid targeting Americans from a site in Iran.

2. Hezbollah, The Qods Force, And Regular IRGC Follow Common Terrorist Techniques, Tactics, And Procedures And Use The Same Terrorist Tradecraft To Ensure Concealment And Cover Worldwide

404. “Tradecraft” refers to the methodologies of engaging in covert operations (including killings) and general espionage. Terrorists and clandestine intelligence operatives both practice tradecraft. The tradecraft rules that govern Hezbollah, the Qods Force, and Regular IRGC are ironclad, inflexible, widely known, and universally applied worldwide, befitting the IRGC’s status as the world’s largest professionalized transnational terrorist organization.

405. **Cover and Concealment.** IRGC tradecraft emphasizes concealment and cover above all other operational imperatives. Both Islamist terrorists and western intelligence officials concur on the core doctrinal point that the two *absolute requirements* for nearly any successful operation are **(i) Concealment**, i.e., something or someone that protects something (or someone) else from being identified; and **(ii) Cover**, i.e., something that provides protection or

¹⁶⁰ Lindemann, *Laboratory of Asymmetry*.

shelter to someone otherwise at risk. Amongst counter-terror professionals, it is axiomatic that “cover” and “concealment” are necessary ingredients in any successful long-term terrorist finance and logistics strategy that depends upon commercial transactions to facilitate terror. Nearly everything a terrorist does requires cover and concealment in some form: meeting with cell members, communicating with leadership, surveilling targets, traveling across an international border to attend a training camp, and so on.

406. Since the IRGC’s founding, Hezbollah, the Qods Force, and Regular IRGC have consistently emphasized cover and concealment as the essential aspect of any successful terrorist operation in light of the unique and affirmative need for the IRGC to “go on offense” and attack Americans abroad. They adhere to cover and concealment as the two most important principles in terrorist tradecraft for a simple reason: the IRGC’s security policy was and is specifically built on paranoid, antisemitic, aggression that explicitly targeted America (by name or in code), and posited that an alliance between Christians (Americans) and Zionists (Israelis) was bent on taking over the Middle East and defiling Islam, such that each member of the IRGC must always be attacking Americans and targeting the U.S. Given the IRGC’s choice of targets, cover and concealment was key to any successful attack.

407. The IRGC (including Hezbollah and the Qods Force) was purposely built for the specific task of attacking America and Israel in order to protect Iran’s Islamic Revolution by staying on a perpetual state of “offense,” i.e., a never-ending campaign of terror against Americans and their allies in the Middle East and around the world designed to strike the “infidels” on their own ground – rather than fight on Iranian soil – via terrorist attacks, usually carried out through a joint cell approach that outsources much of the violence to local IRGC proxies, but always under the control of Hezbollah and the Qods Force.

408. Hezbollah, the Qods Force, and Regular IRGC adhered to the above-described security policy for the purported purpose of preventing “Christians” and “Zionists” from overrunning the Middle East, ending Iran’s Revolution, and forcibly converting every Muslim in the world to Christianity and Judaism. At all times, the Iranian Shareholders with whom MTN Group, ZTE Corp. and Huawei Co. conspired, i.e., fronts for the IRGC (including Hezbollah and the Qods Force), have adhered to this doctrine.

409. The ability of Hezbollah, the Qods Force, and Regular IRGC, to depend upon the reliability of its covers – corrupt corporate partners – was essential to the Conspiracy’s ability to obtain a vast storehouse of American smartphones and network computing technologies.

410. Every principle of terrorist tradecraft practiced by Hezbollah, the Qods Force, and Regular IRGC, begins with **concealment**. The IRGC (including Hezbollah and the Qods Force) has decades of terrorist experience and is the most experienced, practiced terrorist organization in the world today with respect to concealment.

411. Under the “security” doctrine universally practiced at all times by the IRGC, including Hezbollah and Qods Force, IRGC terrorists are taught as a matter of terrorist tradecraft that, if they are faced with a choice between: (a) possibly blowing the concealment of a cover, plot, operative, or transaction, and exposing the IRGC asset in question to capture or detection by the U.S. or Israel, or (b) simply lying, cheating, stealing, defrauding, burning, kidnapping, or murdering their way out of the problem, there is ***no choice at all***: IRGC doctrine commands them to maintain concealment of the asset to prevent discovery. That is, a well-trained Hezbollah, Qods Force, or Regular IRGC terrorist is ***affirmatively compelled*** to do whatever is necessary to maintain concealment as a religious duty, in service of the Islamic Revolution and

the IRGC's holy mandate to "preserve" the Revolution since 1979 by conducting waves of terror campaigns coordinated by Hezbollah's External Security Organization.

412. The IRGC's obsession with preserving concealment underpins this case. Because Hezbollah, the Qods Force, and Regular IRGC, prioritize concealment above all else, an IRGC operative would never truthfully reveal their "security"-related status – i.e., that they were a terrorist operative assigned to the IRGC's Hezbollah Division's External Security Office or through the IRGC's Qods Force and currently on a mission.

413. When a forward deployed terrorist is operating under concealment, as most do, one key challenge involves how to develop reliable partners outside of the terrorist group (e.g., a partner who helps Hezbollah but is not himself a member).

414. Hezbollah, the Qods Force, and Regular IRGC, do not lightly accept foreigners in their terrorist "circle of trust." And the IRGC did not do so here.

415. To earn – and keep – the trust of Hezbollah, the Qods Force, and Regular IRGC, the IRGC insisted that MTN Group and MTN Dubai, and on information and belief, ZTE Corp. and Huawei Co., sign the same IRGC template, in which each Defendant pledged to facilitate the "security" operations of the IRGC, i.e., attacks against Americans worldwide.

416. IRGC concealment doctrine emphasizes an "Orbit" strategy under which the IRGC, including its Hezbollah Division and the Qods Force, structures transactions so that the IRGC is behind one side, one step removed, but fully in control. This IRGC tradecraft is designed to give the IRGC, and its corrupt corporate and financial enablers, the ability to falsely claim that the IRGC did not directly benefit from an otherwise suspect transaction because the counterparty himself was not a member of the IRGC.

417. In 2020, NATO confirmed the IRGC’s “Orbit” strategy in an analysis by Monika Gill, a defense scholar who closely studied how the IRGC deploys communications technology to facilitate anti-American terror, which NATO published in *Defence Strategic Communications*, “[t]he official journal of the NATO Strategic Communications Centre of Excellence.” Gill at 88.

418. According to Ms. Gill’s study, the IRGC’s practices while exercising control of Iran’s heavy construction industry show the IRGC’s “Orbit” strategy as being part of their terrorist tradecraft, because the entire point of the strategy is to enable a future accomplice – like a company that gets caught red-handed – to protest that they have no direct linkage to the IRGC:

The IRGC-CF is comprised of a complex network of Orbit 1 companies and Orbit 2 companies. In Orbit 1 companies, the IRGC-CF is directly represented on the board of directors, whilst in Orbit 2 companies, there ***appears to be no direct representation and therefore, seemingly no links*** to the IRGC-CF. Whilst Orbit 2 companies appear independent of the IRGC, they maintain ties to the directly affiliated companies, and therefore remain under indirect IRGC influence. Baharahn Gostar Kish for example, is an information technology and communications company that has no formal links to the IRGC-CF, with no IRGC members on the board of directors. However, two board members represent Baharahn and ... Gostar, which are both Orbit 1 companies, ***meaning that the company still effectively falls under the IRGC economy.*** (*Id.* at 101-02.)

419. Ms. Gill’s analysis leaves no doubt as to the true nature of Defendants’ counterparties. Indeed, it compels the conclusion that, even now, Defendants’ representations merely further the IRGC Conspiracy. Simply put, it is textbook IRGC terrorist tradecraft to structure deals that are designed to route value to the IRGC even when both sides to the transaction are ***not*** IRGC.

420. The IRGC’s terrorist doctrine emphasizes the reliance upon **cover** through the use of charities, corporations, and endowments, and other ostensibly “civilian” or “economic” entities as covers for Hezbollah, the Qods Force, and Regular IRGC.

421. In recognition of the central role of cover to IRGC doctrine, the IRGC created Unit 400 within the Qods Force. As one regional newspaper explained in 2021:

Unit 400 has a network of facilitators and proxies, including elements in organized crime syndicates. These individuals collect information, make preliminary logistical preparations, and carry out operations if necessary.... Unit 400 has various front companies that both provide cover and money for this terrorist entity to operate.... [T]he IRGC uses its vast network of front companies, religious or charitable organizations around the world to recruit facilitators.¹⁶¹

422. As a consequence, the IRGC, including its Hezbollah Division and the Qods Force, relied upon the importance of using crooked corporate partners to provide “cover” to facilitate, among other things: (i) illicit financial transactions to acquire and distribute U.S. Dollars, e.g., laundering and recycling U.S. Dollar-denominated drug profits to finance Hezbollah operations; (ii) illicit purchases of embargoed American technology, e.g., bulk purchasing thousands of black market secure American mobile phones; (iii) illicit movement of terrorist operatives, e.g., a Hezbollah attack planner whose need to visit Europe requires a visa supplied by a credible front company; (iv) illicit safe havens, e.g., a fictitious company used as cover for an al-Qaeda safehouse in Afghanistan; and (v) illicit cache sites, e.g., a Hezbollah attack planner whose need to visit Europe requires a visa supplied by a credible front company.

423. **Slush Funds For “Off-Books” Terrorist Finance.** Core IRGC doctrine emphasizes that the IRGC, including its Hezbollah Division and the Qods Force, must draw a substantial portion of the funds, arms, personnel, and logistical support for anti-American terrorism globally from “off-books” sources or “slush funds,” with the Bonyad Mostazafan being

¹⁶¹ Shahriar Kia, *Global Terrorist Activities Of The Iranian Mullah Regime*, Weekly Blitz (Bangladesh) (Dec. 4, 2021), 2021 WLNR 39679934.

the most notorious – and important – example. Moreover, “all the IRGC's economic activities are monitored only by internal IRGC auditors and ... the corps pays no taxes.”¹⁶²

424. **Corruption As Terrorist Tactic And Tool.** The terrorist tradecraft practiced and taught by Hezbollah, the Qods Force, and Regular IRGC, have long used corruption, bribery, kickbacks, *khums*, “taxes,” and protection money as a core strategy to facilitate terrorist attacks against Americans in Afghanistan, Iraq, and elsewhere through: (1) terrorist finance, including raising funds, concealing funds, converting funds to U.S. Dollars (the currency of choice for all terrorists), and moving the Dollars to the necessary terrorist cell; (2) terrorist logistics, including acquiring the embargoed technologies necessary to improve the bombs, rockets, communications, and surveillance capabilities necessary to kill or kidnap Plaintiffs; and (3) terrorist freedom of movement, including securing visa and other government papers necessary to a plot, bribing law enforcement to prevent the roll-up of a cell, and the like.

425. Decades of Hezbollah operations, investigations, and prosecutions confirm how Hezbollah, the Qods Force, and Regular IRGC, converted income from the transnational corruption economy for terror, including, but not limited to, examples ranging from Hezbollah’s dominant role in the Lebanese banking system, to Hezbollah’s sponsorship of narcotics trafficking (Hezbollah serves as an elite global management consulting company for narcotraffickers), to Hezbollah’s involvement in transnational organized crime worldwide (where Hezbollah serves as both partner, client, and management consultant).

426. By 2004, Hezbollah, the Qods Force, and Regular IRGC had spent more than two decades developing and refining their shared tradecraft, networks, strategies, and tactics relevant

¹⁶² Rasool Nafisi, *Iran’s Revolutionary Guard Has A Lot To Lose*, Radio Free Europe Documents (Sept. 18, 2009), 2009 WLNR 18604289.

to using corruption as a tool for terror. As a result, Hezbollah, the Qods Force, and Regular IRGC, already had a purpose-built transnational infrastructure enabling them to convert the profits from the “corruption economy” in one country into attacks in that country or others.

427. **Required Donations (Khums) From All IRGC Members.** Shiite theological traditions call for donations (*khums*), usually equal to twenty percent (20%) of a person’s income on every transaction, to support the cause. The IRGC, however, has twisted this religious tradition, like tithing in Christianity, into something else.

428. Under the longstanding IRGC doctrine that Hezbollah teaches to Iranian proxies like Jaysh al-Mahdi, the IRGC emphasizes the need to consistently collect donations (or taxes) as something that is universally required from all profit-generating activities and transactions – *without exception* – including, but not limited to, profits generated through official business, criminal rackets, bribery and kickbacks, and a broad array of other illicit cash flow schemes. The IRGC’s “no exceptions” rule ensures that the terrorist have an administratively simple scheme (analogous to a terrorist flat tax), ensuring ease of implementation, and comporting with the broader IRGC emphasis on its terrorists and proxies embracing administrative simplicity.

429. Under IRGC doctrine, *khums* donations are mandatory on multiple different transaction types, all of which ultimately flow back to fund the IRGC, including its Hezbollah Division and the Qods Force. *First*, if income flows through and IRGC-controlled front (i.e., MTN Irancell) to the IRGC shareholders behind that front, the respective shareholders provide a donation to the others. Thus, for example, if MTN Irancell flowed through \$100 million to the IRGC, one may infer that the IRGC would donate approximately \$20 million to Hezbollah and the Qods Force in order to export Iran’s Islamic Revolution abroad through anti-American terror.

430. *Second*, if an IRGC member (or cutout acting on their behalf) receives an economic benefit, such as a \$400,000 bribe, IRGC doctrine mandates that the bribe recipient kickback, mafia-style, twenty percent of the income to the IRGC. Thus, for example, an IRGC member who receives a \$400,000 bribe could be expected to kickback \$80,000 to the IRGC.

3. Hezbollah's, The Qods Force's, And Regular IRGC's Terrorist Tradecraft And Doctrine Has Historically Relied On Fronts, Operatives, Agents, Cut-Outs, And Orbits To Fund, Arm, And Operationally Aid IRGC Terrorist Proxy Attacks Against Americans

431. The terrorist tradecraft and doctrine of Hezbollah, the Qods Force, and Regular IRGC, reflects a long and notorious history of relying on fronts, operatives, and agents to obtain funding, weapons, and operational support to benefit their terrorist operations and anti-American proxies around the world, most of all Hezbollah.

432. On February 10, 2010, the U.S. Treasury Department announced additional IRGC front-related designations and stated that the IRGC was using illicit commercial transactions to bolster Iran's terrorist enterprise, explaining that "[a]s the *IRGC consolidates control over broad swaths of the Iranian economy, ... it is hiding behind companies ... to maintain vital ties to the outside world*," and that the designations "will help *firms worldwide avoid business that ultimately benefits the IRGC and its dangerous activities*."¹⁶³

433. On August 3, 2010, the U.S. Treasury Department announced additional IRGC- and Qods Force-related terrorist designations that bolstered the U.S. message that the "IRGC and IRGC-QF" provided "Support for Terrorist Organizations," including Hezbollah, and relied upon illicit commercial transactions to fund and arm the IRGC-led terror campaign against Americans:

¹⁶³ U.S. Treasury Dep't, *Treasury Targets Iran's Islamic Revolutionary Guard Corps* (Feb. 10, 2010) (emphasis added).

Today's designations expose Iran's use of ... the Islamic Revolutionary Guard Corps-Qods Force – and state-run social service organizations to support terrorism under the guise of ... economic development

IRGC and IRGC-QF Support for Terrorist Organizations:

The IRGC-QF is the Government of Iran's primary arm for executing its policy of supporting terrorist and insurgent groups. The IRGC-QF provides material, logistical assistance, training and financial support to militants and terrorist operatives throughout the Middle East and South Asia. ... The Government of Iran also uses the Islamic Revolutionary Guard Corps (IRGC) and IRGC-QF to implement its foreign policy goals, including, but not limited to, *seemingly legitimate activities that provide cover for intelligence operations and support to terrorist and insurgent groups. These activities include economic investment ... implemented by companies and institutions that act for or on behalf of, or are owned or controlled by the IRGC and the Iranian government.*¹⁶⁴

434. On December 21, 2010, the U.S. Treasury Department announced additional IRGC-related designations “targeting the financial networks of” the IRGC, and stated once again that IRGC, including Hezbollah and the Qods Force, relied upon illicit commercial transactions, including through bonyads like Bonyad Mostazafan, to facilitate Iran's terrorist enterprise:

The IRGC continues to be a primary focus of U.S. ... sanctions against Iran because of the central role it plays in Iran's ... support for terrorism The U.S., UN, EU, Japan, South Korea and others have all targeted the IRGC for sanctions because of this illicit activity. With the IRGC's expanding influence and control over broader segments of [Iran's] economy ... increasing numbers of Iranian businesses are subsumed under the IRGC's umbrella and identified with its illicit conduct. ... [B]onyads are opaque, quasi-official organizations controlled by key current and past [Iranian] officials and clerics. Bonyads receive [government] benefits ... but are not required to have their budgets publicly approved. They account for a significant portion of Iran's non-petroleum economy. ... Treasury has designated 14 IRGC-affiliated individuals and entities since June 2010 for facilitating Iran's nuclear [] program or support for terrorism.¹⁶⁵

¹⁶⁴ U.S. Treasury Dep't, *Fact Sheet: U.S. Treasury Department Targets Iran's Support for Terrorism Treasury Announces New Sanctions Against Iran's Islamic Revolutionary Guard Corps-Qods Force Leadership* (Aug. 3, 2010) (emphasis added).

¹⁶⁵ U.S. Treasury Dep't, *Fact Sheet: Treasury Designates Iranian Entities Tied to the IRGC and IRISL* (Dec. 21, 2010).

435. On June 23, 2011, the U.S. Treasury Department announced additional IRGC-related designations that reinforced the U.S. message that illicit transactions with IRGC commercial fronts directly aided terrorism against Americans by Iranian terrorist proxies:

Treasury Targets Commercial Infrastructure of IRGC, Exposes Continued IRGC Support for Terrorism. Today, ... Treasury took action to designate ... Iranian commercial entities ... owned by [IRGC] ... The IRGC continues to be a primary focus of U.S. and international sanctions against Iran because of the central role it plays in ... Iran's illicit conduct, including Iran's ... support for terrorism ... As Iran's isolation has increased, the IRGC has expanded its reach into critical sectors of Iran's economic infrastructure – to the detriment of the Iranian private sector – ***to generate revenue and conduct business in support of Iran's illicit activities.*** Today's actions target core commercial interests of the IRGC, while also undermining the IRGC's ability to continue using these interests to facilitate its ... illicit conduct. ... The IRGC has a growing presence in Iran's financial and commercial sectors and extensive economic interests ..., controlling billions of dollars in corporate business. Given its increased involvement in commercial activity, imposing financial sanctions on commercial enterprises of the IRGC has a direct impact on revenues that could be used by the IRGC to facilitate illicit conduct.¹⁶⁶

E. In Furtherance Of The Conspiracy, Hezbollah, The Qods Force, And Regular IRGC Managed A Transnational Network Of Terrorist Finance, Logistics, Operations, And Communications Cells To Fund, Arm, Logistically Sustain, And Facilitate Attacks On Americans In Afghanistan

436. **United States.** Hezbollah, the Qods Force, and Regular IRGC rely upon a global network of cells, operatives, cover companies, and allied criminals in the corporate world (like Defendants) and the criminal world (like narcotraffickers and transnational crime organizations).

437. Hezbollah, the Qods Force, and Regular IRGC, operated the Conspiracy in the same manner as a multinational corporation, seeking to leverage geographic efficiencies, networks, and distributed competencies to maximize the lethality of the Conspiracy's terrorist campaigns against Americans in Afghanistan, Iraq, Yemen, Syria, Europe, Pakistan, and

¹⁶⁶ U.S. Treasury Dep't, *Fact Sheet: Treasury Sanctions Major Iranian Commercial Entities* (June 23, 2011) (emphasis added).

elsewhere. This section briefly outlines how Hezbollah, the Qods Force, and Regular IRGC, leveraged terrorist finance, logistics, technical and communications support from around the world to directly aid the terror campaign against Americans in Afghanistan.

438. ***American Technologies.*** Hezbollah, the Qods Force, and Regular IRGC depended upon the IRGC's ability to access technologies, markets, and systems that were found exclusively in the United States to execute key parts of the Conspiracy. Simply put, they needed as much access to America as possible to kill as many Americans as possible.

439. Hezbollah, the Qods Force, and Regular IRGC relied upon American-designed, protected, manufactured, and/or assembled technologies, including, but not limited to, mobile phones, smartphones, enterprise servers, networking technologies, and software, because they are the gold standard. No other country made a credible competing device (that was available to the public, as opposed to their own "security" agencies) between 2001 and 2022.

440. ***American Markets.*** Hezbollah, the Qods Force, and Regular IRGC relied upon in-person and online sales markets in the United States, including but not limited to currency markets (relying upon the U.S. Dollar as the IRGC's preferred currency) technology markets (relying on U.S. goods as the IRGC's preferred technology source), financial markets (relying on U.S. financial markets because U.S. banks have connectivity to the 50+ countries where Qods Force and Hezbollah operate), labor markets (relying on skilled laborers, particularly information technology consultants, to service the IRGC's illicitly acquired U.S. technologies), and black markets (relying on the ability to acquire some of the above items available only in the U.S.).

441. In every instance, Hezbollah, the Qods Force, and Regular IRGC depended upon their ability to access U.S. markets at home to kill Americans abroad because U.S. markets have unique power to set the terms and pricing for the world, and were often also the only location

where Hezbollah, the Qods Force, and Regular IRGC could acquire key items in the covert manner needed under the IRGC's terrorist tradecraft. For example, the IRGC could not source large amounts of U.S. Dollars or access state-of-the-art American technologies without the IRGC, or one of its corporate co-conspirators, reaching into the U.S. to further the Conspiracy. This case concerns the various nodes and modalities by which the IRGC accomplished that.

442. ***American Systems.*** Hezbollah, the Qods Force, and Regular IRGC relied upon their ability to access certain financial, technical, and knowledge systems that were stored exclusively inside the United States. For example, the IRGC depended upon the ability of its terrorist computer programmers to access certain proprietary databases located inside of the United States to complete the design of a part necessary for a new type of bomb.

443. **U.A.E.; Iraq; Iran; Lebanon; Yemen; Syria; Afghanistan; Pakistan.** From 9/11 through the present, attack planners, logisticians, and financiers for Hezbollah, the Qods Force, and Regular IRGC as well as nearly every other major Islamist terrorist group, including but not limited to al-Qaeda, the Taliban (including its Haqqani Network), and others, have relied upon the U.A.E., especially Dubai, as a logistical, financial, and operational hub, where they could organize their terrorist campaigns in Iraq, Iran, Lebanon, Yemen, Syria, and Afghanistan.

444. With respect to the IRGC's terrorist campaign against Americans in Iraq and Syria in furtherance of the IRGC Conspiracy, the U.A.E. served as a logistical, financial, and operational hub for the campaign, and the U.A.E. was functionally part of one interlocking geography of extreme terrorist finance and logistics risk and hub of activity,¹⁶⁷ purpose-built for

¹⁶⁷ For the avoidance of all doubt, the government of the U.A.E. was, and remains, an ally of the U.S. in the fight against terrorism. The terrorists' use of the U.A.E. as a hub was based on a range of other factors, including, but not limited to, geography, history, particular trading networks, transportation channels, and an advanced infrastructure for conducting transactions

the IRGC Syndicate Terrorist Proxies' terror campaigns. Simply put, the terrorists did not respect the borders of any of these countries – other than Iran and Syria, with whom they were allied, rendering the issue moot – and viewed the entire geography as one combined theater.

445. **South Africa.** Hezbollah, the Qods Force, and Regular IRGC have long operated openly in South Africa. “Iran and South Africa have cooperated on a number of fronts in recent decades, including at the U.N., where South Africa has at times advocated for Iran” and “[t]he pair also have a military relationship.”¹⁶⁸

446. The IRGC's freedom of movement in South Africa is a legacy of Ayatollah Khomeini, who stood against the Apartheid regime while, unfortunately, the United States (for a time) did not. For decades, Hezbollah, the Qods Force, and Regular IRGC leveraged Iran's historical opposition to Apartheid. Because of this unique Iranian-South African history, Hezbollah, the Qods Force, and Regular IRGC viewed South Africa as a veritable home away from home, as South Africa was one of the few major democracies to abstain from joining the sanctions regime against Iran and to afford the IRGC relatively unfettered freedom of movement. As a result, Hezbollah, the Qods Force, and Regular IRGC operated clandestine fundraising, logistics, and operations networks in South Africa for decades.

447. In an interview with *Politico*, American intelligence officials confirmed that “[t]he Iranian government [] operate[d] clandestine networks in South Africa,” “and has had a foothold there for decades.” In 2015, *Al Jazeera* and *The Guardian* reported on leaked intelligence documents revealing an extensive network of Iranian operatives in South Africa.

and moving goods and monies throughout the Middle East. The terrorists, like many multinational corporations, set up their regional headquarters in Dubai for these reasons.

¹⁶⁸ Nahal Toosi and Natash Bertrand, *Officials: Iran Weighing Plot To Kill U.S. Ambassador To S. Africa*, *Politico* (Sept. 13, 2020).

448. According to leaked documents from the South African intelligence service, Hezbollah and the Qods Force operate cells in South Africa, showing “confirmed” links between Iranian operatives in overseas embassies and “terrorists.”

449. In or about 2020, American intelligence services detected that Hezbollah, the Qods Force, and Regular IRGC was planning a terrorist attack in South Africa to kill the U.S. ambassador to South Africa as retaliation for the killing of Qassem Soleimani in January 2020. Hezbollah’s choice of South Africa as the potential attack site is revealing, as the terrorists had the chance to survey all the world to choose the best location to kill an American ambassador. As *Politico* noted, the U.S. ambassador to South Africa “may also [have] be[en] an easier target than U.S. diplomats in other parts of the world, such as Western Europe, where the U.S. ha[d] stronger relationships with local law enforcement and intelligence services.” *Id.*

450. **Europe.** Europe has long been a hub for terrorist finance, logistics, and operational support for Hezbollah, the Qods Force, and Regular IRGC as well as al-Qaeda, the Taliban, and their Syndicate terror partners in Afghanistan and Pakistan. Europe’s proximity to many of the attack theaters and ease of travel make it a key site for the terrorist campaign.

451. **The Americas.** The IRGC, through Hezbollah and the Qods Force, maintains a substantial presence in the Americas, including, but not limited to, in Venezuela, Colombia, Paraguay, and other nations.

452. Hezbollah and the Qods Force maintained operational, finance, and logistics cells in multiple nations in the Americas, through which Hezbollah operated an array of criminal schemes, e.g., narcotics trafficking, to repatriate money back to the terrorist campaign.

453. Hezbollah and the Qods Force support the terrorist campaign in the Middle East from their cells in the Americas. Indeed, that is the purpose of the cells far from Hezbollah's home in Beirut – cash and logistics flow for its terror campaigns.

454. **Southeast Asia.** The IRGC, through Hezbollah and the Qods Force, maintains a substantial presence in Southeast Asia.

455. Hezbollah and the Qods Force maintain operational, finance, and logistics cells throughout multiple Southeast Asian nations, including Malaysia and Singapore.

456. Hezbollah and the Qods Force support the terrorist campaign in the Middle East from their Southeast Asian cells. Indeed, that is the purpose of the cells far from Hezbollah's home in Beirut – cash and logistics flow for its terror campaigns.

IV. THE CONSPIRACY DEPENDED UPON THE CO-CONSPIRATORS' ROBUST ACCESS TO U.S. TECHNOLOGY, U.S. DOLLARS, AND U.S. PERSONS TO CARRY OUT ATTACKS AGAINST AMERICANS IN THE MIDDLE EAST

A. After The U.S. Invasions Of Afghanistan And Iraq, Hezbollah, The Qods Force, And Regular IRGC Concluded That They Needed To Revolutionize Their Access To U.S. Technologies Through Corrupt Corporate Partners

457. By 2003, the tech-gap between the “security” operatives deployed by Hezbollah, the Qods Force, and Regular IRGC on the one hand, and U.S. counter-terrorists, law enforcement, and intelligence officers, on the other, was so vast it was as if Americans and the IRGC “security” operatives targeting them experienced two different technological realities.

458. After the fall of Saddam Hussein in 2003, U.S. personnel in the Middle East practiced their counter-terror tradecraft in one reality where Americans wielded expansive 24/7 surveillance powers, possessed unparalleled intelligence networks, and had real-time data analytic abilities that played a key role in reducing the threat of Islamist terror.

459. Meanwhile, the IRGC “security” operatives practiced their tradecraft in a world that was upside down and terrifying. A sloppy phone call could result in a precision American

airstrike a few minutes later. An errant text message could enable the “Great Satan” to take down a Joint Cell. A carelessly documented transaction could reveal an important laundering scheme. Most of all, the “security” operatives of Hezbollah, the Qods Force, and Regular IRGC were caught in a digital cage from which they could not carry out their religious, and constitutionally prescribed duty – attack and kill Americans.

460. The IRGC knew that the U.S. telecom and network computing industry would not solve their problem – if anything, the American industry would only widen the gap even more between the IRGC and the Americans it wanted to kill. For decades, large U.S.-headquartered telecom and network computing companies have been reliable partners of the U.S. government with respect to reducing the threat from terrorism. Indeed, the anti-terrorism track record of America’s telecommunications and network computing companies has been among the best of any industry anywhere in the world.¹⁶⁹

461. This matters because the robust commitment of American telecom and network computing companies to anti-terrorism compliance was known to the IRGC (and all other industry participants), which meant that the terrorists knew they would be unable to count on their normal strategy for illicitly acquiring something – bribery, extortion, fraud – because none of those strategies held the promise of success at the industrial scale that Hezbollah, the Qods Force, and Regular IRGC required for their global terrorist Conspiracy against Americans.

462. By 2003, the IRGC knew that its operatives would never be able to sustain the global terrorist Conspiracy it had planned against America after 9/11 unless the IRGC could find

¹⁶⁹ Plaintiffs are not aware of any federal criminal terrorism-related prosecutions, civil Anti-Terrorism Act allegations, or analogous anti-terrorism matter brought by any government against any such large U.S.-headquartered telecom and/or network computing companies.

a way to break out of the digital detention cell that was effectively created by the walls of compliance offered by America's telecommunications and network computing companies.

463. Hezbollah ordinarily serves as the IRGCs illicit procurement agent of choice for a litany of reasons including, but not limited to, deniability, cultural affinities, and the presence of a Lebanese diaspora dispersed around the world, upon which Hezbollah, like most Islamist groups, heavily relies.

464. By 2003, the IRGC had tasked Hezbollah with solving a riddle: how do they, the terrorists, establish the reliable, secure, and covert pipeline that they need to illicitly acquire the tens of thousands of state-of-the-art American smartphones and network computing technologies *each year* necessary to sustain their decades-long, global terrorist campaign against America?

465. The answer? Identify potential multinational corporate partners who would be willing to provide the technology they needed.

466. As the IRGC spun up its transnational terrorist Conspiracy, its leadership worked with Hezbollah and the Qods Force to develop a comprehensive plan to revolutionize their respective terrorist capabilities to prepare for their anticipated decades-long terrorist campaign against Americans throughout the Middle East. To accomplish the object of the Conspiracy – ejecting the United States from the entire Middle East through a campaign of terror – the terrorists had several critical requirements.

467. *First*, the IRGC and its terrorist allies needed a generational upgrade in the security of their computer systems and network technologies, especially the state-of-the-art American servers that were *the* condition precedent for the IRGC's ability to execute a Revolution in Terrorist Affairs (a terrorist mirror image of the US military's Revolution in Military Affairs) (see *infra* ¶ 313), and without which the IRGC's efforts would be less

effective, less efficient, more expensive, and would produce, ultimately, fewer dead Americans.

Given the sheer scale of the IRGC's terrorist Conspiracy, even marginal improvements in IRGC computing power translated to more plots being shared, more fundraising solicitations, more recruits, and ultimately, more attacks.

468. *Second*, the IRGC and its terrorist allies needed a reliable, replenishable, untraceable source of suppliers for illicit high-quality American mobile phones sold inside the United States and then illegally reexported to eventually flow through the Qods Forces logistics channels – as intended – before reaching Hezbollah, who relied upon American phones to coordinate Iran's global terrorist Conspiracy against Americans in Afghanistan and Iraq.

469. Given the transnational nature of the IRGC Conspiracy, Hezbollah, the Qods Force, and the leadership of terrorist proxies like Jaysh al-Mahdi (in Iraq) and the Taliban (in Afghanistan), faced a simple, but potentially fatal, problem confronting their post-9/11 terrorist enterprise against America: how to facilitate the free movement of key terrorist leaders, attack planners, fundraisers, and logisticians between the various hubs of the Conspiracy, e.g., a senior Hezbollah operative who shuttles from Beirut (where Hezbollah is based), to Syria (where Hezbollah and the IRGC maintain a listening post), to Baghdad (where Hezbollah led Joint Cells targeting Americans), and then to Tehran (where the IRGC is based). This isn't the plot of a spy movie: it describes the ordinary travel patterns of thousands of IRGC terrorists each year.

470. The IRGC understood that, in the modern era of terrorism, without a reliable supply of secure mobile phones, its Hezbollah and Qods Force operatives were at an enormous disadvantage, unable to move and communicate freely for fear their phones were compromised by the Americans (as they likely were).

471. Worse, the IRGC lacked any easy solutions because America dominated the mobile phone industry and was not open for business to the IRGC. Shut off from the U.S. marketplace, the IRGC was unable to build their own phones and unwilling to place the lives of their most prized operatives – the people who led joint cells and coordinated operations – in the hands of the junky, unreliable mobile phones being made outside of the United States at the time.

472. Thus, the IRGC embarked on a comprehensive strategy designed to achieve its technological revolution, obtain reliable industrial scale supplier relationships that could source American mobile phones, close the communications gap with the “Great Satan,” and enhance the lethality of its global terrorist campaign against America. To do so, the IRGC needed to source tens of thousands of untraceable mobile phones *every year* to ensure the secure and untraceable lines of communication between combined cells of Hezbollah, Qods Force, and local proxy terrorist allies operating in dozens of countries worldwide and, among other people, their local organized crime allies (e.g., narco-traffickers), corrupt politicians (essential for things like passports and permits), and terrorist headquarters, as examples.

473. Unfortunately for Hezbollah, the Qods Force, and Regular IRGC who were responsible for the Conspiracy’s transnational logistics, weapons, financial, personnel flows, they could not source the tens of thousands of advanced American smartphones they needed every year with a few purchase orders on Bonyad Mostazafan’s letterhead, because the IRGC terrorists the Bonyad was designed to benefit, e.g., Hezbollah and the Qods Force, were sanctioned. Even if the Regular IRGC were not sanctioned, as a matter of IRGC terrorist tradecraft, lawful purchases of American phones inside U.S. markets by the precious Hezbollah or Qods Force assets inside the United States (for whom exposure was not to be risked lightly), while viable in small increments, was impossible at the commercial scale necessary for the

Conspiracy to succeed. Moreover, direct purchases by Hezbollah or Qods Force assets themselves would leave an evidentiary paper trail and risk the terrorists' operatives being compromised – a potential catastrophe for Hezbollah, the Qods Force, and Regular IRGC.

474. Logically, that left the IRGC in a predicament. The IRGC could only satisfy its operational requirements through the bulk acquisition of thousands of high-end American mobile phones every year, but if the IRGC attempted to do so directly, even using existing IRGC front companies, the enterprise would not yield nearly enough American phones, because the black market cell phone trade is a volume business where deals and goods must move rapidly. Thus, the IRGC needed front companies that offered the agility, resources, global networks, and executives with willingness to aid the world's worst terrorists for profit.¹⁷⁰

475. Accordingly, the IRGC's ability to prosecute a global terrorist campaign against the United States required the services of corrupt multinational corporate partners, with deep resources, large logistics chains, and a willingness to conspire with anti-American terrorists. The following characteristics were key:

- (i) **New terrorist cash flow** generated by taking over a “civilian” company, to make it *easier* to illicitly acquire American technology (that's the point of cover) and make it *harder* for the IRGC's enemies to mobilize effective sanctions against the funding source (because IRGC apologists, like MTN Group, could publicly spread disinformation to undermine any pressure campaigns, as MTN Group did, and continues to do to this day);
- (ii) **Illicit acquisition of critical American technologies**, including secure American smartphones, computer networking technology, and other sensitive dual-use American technologies to accomplish the IRGC's own Revolution in Terrorist Affairs; and the

¹⁷⁰ Because the global market for the sale of illegal American smartphones was vulnerable to law enforcement shocks that could rapidly suppress (temporarily) the supply chain – e.g., a raid in Detroit that removed one of the largest dealers from servicing the black market – it was imperative for the IRGC that its purchasing agents have the agility, financial resources, and global assets to source illicit American-exported cell phones in black markets worldwide, including, but not limited to, illicit cell phone markets on every continent but Antarctica.

- (iii) **Robust logistics capabilities** befitting the operation of Hezbollah, the Qods Force, and Regular IRGC as a multinational terrorist corporation that had a constant need to manage and rationalize the flow of illicit funds, arms, communications, narcotics, and personnel across six continents, all in support of the shared terrorist enterprise.

476. At bottom, decrepit telecommunications, network computing, and associated technologies posed an immediate, and dire, threat to the IRGC's ability to kill as many Americans as possible in Afghanistan and Iraq because the IRGC was generations behind its U.S. enemies on nearly every key class of communications and computing technologies necessary to sustain a modern global terrorist campaign stretching from Syria to Afghanistan.

477. The "Revolution in Military Affairs" or "RMA" refers to a widely accepted military hypothesis that emerged in the 1990s and posited that Western militaries needed to prepare for future asymmetrical threats by maximizing the technological gap between Western militaries and local hostile forces, e.g., IRGC proxies in Afghanistan, to achieve objectives such as increasing the speed with which forces can maneuver, increasing the flow of intelligence to troops, facilitating real-time information sharing amongst allied friendly forces, and promoting "interoperability" between the militaries of different nations.

478. By early 2004, the IRGC Conspiracy was in full bloom. Hezbollah, the Qods Force, and Regular IRGC had embraced their own take on the RMA, but repurposing its principles for use by Iran-backed terrorists, e.g., a Revolution in Terrorist Affairs. The IRGC concluded that it had to overhaul the terrorists' communications, computing, internet, and cyber capabilities to enable Iran to continue aiding attacks against Americans in Afghanistan and Iraq.

479. The IRGC had no choice but to seek American technology because America held the dominant position with respect to the world's computers, mobile phones, servers, routers, and the like, and the IRGC understood that it needed to illicitly acquire vast amounts of embargoed American technologies to commit terrorist attacks.

480. By late 2004, the IRGC was desperate to upgrade its telecommunications because it understood that its ability to help kill and maim Americans at scale in Iraq, Afghanistan, and elsewhere depended upon the ability of its Hezbollah and Qods Force operatives, and their proxies to solve their American mobile phone access crisis. The IRGC's terrorist proxy Jaysh al-Mahdi was routed by U.S. forces twice that year. Moreover, the escalating gap between American counter-terrorists and IRGC "security" operatives, i.e., Hezbollah and Qods Force terrorists, threatened to eviscerate the ability of Hezbollah, the Qods Force, and Regular IRGC to facilitate terrorist violence against the United States in Afghanistan and Iraq.

481. Indeed, the IRGC watched, with escalating alarm, as its communications and computing gap widened and threatened its ability to attack and kill Americans in Afghanistan and Iraq. The need to find a long-term technology supply fix and was one of the highest priorities of Hezbollah, the Qods Force, and Regular IRGC.

B. The IRGC Addressed The Conspiracy's Funding And Logistics Needs By Seizing Iran's Largest Telecommunications Companies To Acquire The Technologies, Cash Flow, And Logistical Aid From Corporate Partners

482. In 2004, the IRGC embarked on a two-step solution. *Step One:* the IRGC seized Iran's large state-owned telecom companies and converted them into tools of terrorist finance, logistics, propaganda, recruiting, and operations. In 2005, "Ayatollah Khamene'i issued a decree ... ordering 25% of state-owned assets to be privatised within 5 years. \$120 billion worth of government assets were sold ... Yet, the *largest purchaser of privatised government assets was the IRGC*, which received favourable terms from the Ahmadinejad regime. Under the *guise* of de jure privatisation, state-owned assets were *de facto militarised*." Gill, *supra*, at 104.

483. *Step Two:* the IRGC secured the agreement of complicit, corrupt telecommunications companies, including ZTE Corp., Huawei Co., and co-conspirators MTN Group and MTN Dubai, which were willing to do business with fronts for the IRGC's

transnational terrorist logistics, technology, and financial enterprise and help the terrorists illicitly source the comprehensive suite of state-of-the-art American technologies that the IRGC determined were necessary for its own Revolution in Terrorist Affairs, so that Hezbollah and the Qods Force could do what they ended up doing: launch a devastating wave of violence against Americans throughout Afghanistan and Iraq.

484. The IRGC's two most important telecom front company targets were MTN Irancell and TCI, and the IRGC quickly assumed full control of both companies, completely converting each to its terrorist enterprise.

1. MTN Irancell

485. In 2004, the IRGC negotiated with Turkcell, a Turkish mobile phone company, hoping Turkcell would be the corrupt corporate partner the IRGC required to extract a vast digital armory of embargoed American technologies. As negotiations progressed, however, it became clear that while Turkcell was willing to help build a modern Iranian phone system, it was not willing to provide direct "security" assistance to the IRGC.

486. MTN Group and MTN Dubai had no such scruples. Sensing weakness in the IRGC's negotiations with Turkcell, MTN Group and MTN Dubai hatched a comprehensive plan, which they internally called "Project Snooker," designed to steal the Irancell license from Turkcell – and the billions of dollars in profits that would flow to MTN Group and MTN Dubai thereafter. Ms. Gill explained the result:

the *IRGC asserted their role* in the communications economy through two significant developments in telecommunications infrastructure involving MTN Irancell and TCI. MTN Irancell was launched in 2005, at the start of Ahmadinejad's presidency, as a ... joint venture between ... MTN Group and the Iran Electronic Development Company (IEDC). A subsidiary company of the Iranian Ministry of Defence, IEDC maintained *close ties with the Revolutionary Guard. Following the IRGC's opposition* to foreign involvement in Iran's strategic telecommunications sector, IEDC negotiated 51% ownership of the

MTN Irancell joint venture, ensuring that *the military had a majority stake in the newly formed telecommunications infrastructure*. (Gill, *supra*, at 105.)

487. In her article documenting how the IRGC converted MTN Irancell and TCI into tools of terrorist finance and logistics published by NATO, Ms. Gill explained:

By *militarising, rather than privatising the economy*, the regime transferred ownership from ‘relatively transparent parts of the public sector to *other parts of the public sector shielded from public scrutiny*’, *such as the Revolutionary Guard*. It is in this *fictional separation between the public and private sector in Iran that the invisible hand of the IRGC can be assessed*. *Power projection and realpolitik* remained central to the Guard’s strategic thinking to the same extent as their ideological devotion. *Id.* at 108-09 (emphases added).

488. The IRGC’s takeover of MTN Irancell and TCI produced a financial windfall for Hezbollah, the Qods Force, and Regular IRGC. Ms. Gill explained that:

From a business perspective, the IRGC ... create[ed] a military-commercial complex in which the Guard benefitted from the construction of a perceived and persistent threat. ... Whilst publicly promoting rhetoric about national security and the defence of Shi’ite Islamic culture, the IRGC was *sustaining a military-commercial complex that benefited them financially*. The IRGC and the Iranian communications economy maintained a *close partnership*, with both taking advantage of the articulation of a soft war. ...[T]here [was] a notably profit-driven motive to the Guard’s economic involvement. ... the involvement of the IRGC in the communications economy under Ahmadinejad was reflective of an ideological, but also increasingly opportunistic Revolutionary Guard. *Id.* at 110-111 (emphasis added).

489. “[T]he IRGC became a moneymaking machine” after it deliberately blended the commercial and terrorist functions of MTN Irancell and TCI to ensure that Hezbollah, the Qods Force, and Regular IRGC could use MTN Irancell and TCI revenues to furnish off-books cash to, among other things, keep former members of Hezbollah, the Qods Force, and Regular IRGC on the IRGC’s payroll. According to Ms. Gill,

The IRGC acts as a business fraternity within which members of the Guard can progress along a prescribed career path. Following active service, IRGC members are offered senior positions in state-affiliated media organisations and telecommunications networks *such as IRIB, TCI, and MTN Irancell*. *Accordingly, ‘no one ever leaves the IRGC’*; its senior officers are viewed as an

Iranian ‘freemasonry’ and ‘Ivy League network’, signalling that the IRGC exceeds ideological devotion. ... When ‘privatising’ the national media and telecommunications infrastructure, the Ahmadinejad regime sold its majority stake to the IRGC, ***blending its mission of national security with ‘investor profits’***. In holding senior economic positions in communications infrastructure companies and accruing profits, ***the IRGC became a ‘moneymaking machine’***. ... The IRGC’s opportunistic and exploitative involvement in the communications economy facilitated a system of military crony capitalism within Ahmadinejad’s Iran. ... The IRGC ***grew to depend on the communications economy to support the personal and financial endeavours of the Guard***, who valued safeguarding their own self-interest to the same extent as they valued safeguarding the revolution. (*Id.* at 111-12.)

490. In sum, according to Ms. Gill, “the IRGC as an institution was reliant on the communications economy as a source of capital gain” and “the IRGC used the fictional separation between the public and private sectors in Iran to facilitate its rise as an economic conglomerate.” *Id.* at 112. At bottom, according to Ms. Gill, the IRGC’s control over MTN Irancell and TCI was not just about propaganda – the IRGC depended upon such control to support its “security” agenda, i.e., anti-American terror by using the fronts to raise money:

whilst the Guard relied on the communications economy to propagate their ideology, they also ***acquired and monopolised*** communications infrastructure as a ***source of capital gain***. The Guard’s involvement with the communications economy moved beyond the projection of revolutionary ideology, becoming equally a matter of realpolitik and of ***accruing military capital***. (*Id.*)

2. Telecommunications Company Of Iran (TCI)

491. In 2009 – four years after the IRGC’s strategy to illicitly source terrorist material through Irancell relied upon “using IEDC as a front” in the IRGC’s 2005 agreement with MTN Group – the IRGC emerged from its previous position of cover on Irancell to publicly assume a majority stake in Iranian telecom company, TCI. According to Ms. Gill,

[I]n September 2009, shortly after the violent protests following Ahmadinejad’s re-election, the government announced plans to privatise TCI. Amongst the investors were ***numerous IRGC-backed institutions***, including the IRGC-CF, the Mostazafan Foundation, and the Execution of the Imam’s Order company. Minutes after TCI was privatised, ***the IRGC acquired 51% of the company*** in a \$5 billion deal—the ‘largest trade in the history of the Tehran Stock Exchange’.

This represented *‘yet another calculated step’ in the IRGC’s campaign to dominate Iran’s communications economy. Rather than using IEDC as a front, as they had done in 2005, the IRGC had overtly purchased a majority stake in TCI’s monopoly over Iranian telecommunications. (Id. at 105-06.)*

V. DEFENDANTS FURTHERED THE CONSPIRACY AND TRANSACTED BUSINESS WITH FRONTS, OPERATIVES, AND AGENTS CONTROLLED BY HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC

492. MTN, ZTE, and Huawei did business with fronts, agents, and operatives for Hezbollah, the Qods Force, and Regular IRGC.

493. The IRGC controlled the entire Iranian telecom sector from top to bottom. The following Iranian fronts, operatives, and agents played especially prominent roles in ensuring that any telecom transactions in Iran benefited the IRGC’s, including Hezbollah’s and the Qods Force’s, global terrorist agenda.

A. The Bonyad Mostazafan

494. The Bonyad Mostazafan, also known as the *Bonyad Mostazafan va Janbazan*, Mostazafan Foundation, and Alavi Foundation (herein, the “Bonyad Mostazafan”), was established after the Islamic Revolution to steal and manage property, including that originally belonging to religious minorities in Iran such as Baha’is and Jews, to fund the export of the Iran’s Islamic Revolution around the world.

495. The Bonyad Mostazafan was and is an IRGC, including Hezbollah and the Qods Force, front. The Bonyad Mostazafan’s purpose was and is to raise funds and obtain weapons and components) for the IRGC’s, including Hezbollah’s and the Qods Force’s, terrorist operatives and proxies like al-Qaeda and the Taliban. Funds and weapons (including weapons components) provided to the Bonyad Mostazafan through its commercial transactions inevitably flowed through Irancell and TCI to Hezbollah and the Qods Force and, through them, to IRGC

proxies al-Qaeda and the Taliban, to fund and arm al-Qaeda and Taliban attacks against Americans in Afghanistan from 2007 through the present.

496. At all times, the Bonyad Mostazafan has been led by an agent or cut-out for Hezbollah, the Qods Force, and Regular IRGC and has served as a central hub of IRGC, including Hezbollah and the Qods Force, fund raising, weapons development and acquisition, computing, and communications infrastructure for Iran's terrorist enterprise, which value has flowed through the IRGC to al-Qaeda and the Taliban.¹⁷¹

497. The Bonyad Mostazafan is currently led by IRGC Brigadier General Parviz Fattah, who is also, on information and belief, a Qods Force operative.

498. The Bonyad Mostazafan has been widely understood in business, diplomatic, military, and media circles to be a front for Iranian terrorism through Hezbollah, the Qods Force, and Regular IRGC since the 1990s.

499. On May 28, 1995, the Bonyad Mostazafan's status as an Iranian terrorist front made international news when *Newsday* – in an article republished around the world through various affiliate relationships – reported that the Bonyad Mostazafan served as a front for raising money and sourcing weapons for Iran's terrorist proxies, including Hezbollah:

[I]n a four-month investigation based on dozens of interviews with law-enforcement officials and U.S. government specialists, knowledgeable Iranians who support the regime as well as dissidents, and public and private documents, *Newsday* has found that:

- [The Bonyad Mostazafan] ... is controlled by Iran's clerical leadership, federal officials say.
- Several of [the Bonyad Mostazafan's] current and former officers and directors have been ***implicated in arms and technology shipments to***

¹⁷¹ For example, Mir Hossein Mousavi, who directed the Bonyad Mostazafan for almost a decade, was "the Butcher of Beirut," played a key role in Hezbollah's leadership council and in its attacks on Americans in Lebanon, including the 1983 Marine barracks bombing.

Iran, and a former president of the foundation allegedly tried to ship germ-warfare agents to Tehran, according to these officials.

- [The Bonyad Mostazafan] *served as a front* ... for the placement of agents from the Revolutionary Guard, dedicated zealots who ... spy and *obtain military technology* from the United States and abroad.
- [The Bonyad Mostazafan] finances [entities] in the United States that support Iran's militant version of Islam and provides safe haven for groups and individuals supporting the Islamic terrorist group[] ... *Hezbollah*. ...

In a classified report ... the FBI asserted that [the Bonyad Mostazafan] was “entirely controlled by the government of Iran,” which *used [the Bonyad Mostazafan] to set up “covert subbranches disguised* as educational centers, mosques and other centers.” ... The FBI report, according to a U.S. official, claims that [the Bonyad Mostazafan] *funds “fundamentalist extremist groups”* and that Iranian students who received scholarships from [the Bonyad Mostazafan] to study in the United States *“gather[ed] intelligence”* ... and *collected “technical and scientific information” for the Iranian regime*.

In 1989, Oliver Revell, then the No. 2 official at the FBI, told the Senate terrorism subcommittee that some of the “students” receiving [the Bonyad Mostazafan] grants were in fact Revolutionary Guard agents. ... Revell ... said much of [the Bonyad Mostazafan]’s funds go to “a great number of mosques (in the United States) . . . where there are *organizations which directly support Hezbollah...[,]*” an Iranian-supported militant group ... that has launched terrorist attacks under the tutelage of the Revolutionary Guards. ... *The [Bonyad Mostazafan] is administered by Mohsen Rafiqdoost, founder of the Revolutionary Guards*. Rafiqdoost reports only to the Ayatollah Ali Khamenei, Iran’s spiritual leader.

Knut Royce and Kevin McCoy, *Militants Build On Iranian Foundation*, *Newsday*, republished by Pittsburgh Post-Gazette (May 28, 1995), 1995 WLNR 2452536 (emphasis added).¹⁷²

500. In the same investigative report, *Newsday* also disclosed that “U.S. and European officials say that [the Bonyad Mostazafan] has long been a front for the procurement of military

¹⁷² After the Islamic Revolution, the Ayatollah seized what had previously been the Alavi Foundation and merged it with the Bonyad Mostazafan. Thereafter, they were one and the same and always were indistinguishable and different names for the same Iranian terrorist front. *See, e.g., id.* (“Vincent Cannistraro, who left the CIA in 1990 as a top official of its counterterrorism center, said in a recent interview, ‘The [Bonyad Mostazafan] and the Alavi Foundation are the same, under different names.’ Other U.S. officials agreed.”).

goods and prohibited technology for Iran, particularly for the Revolutionary Guards.” Knut Royce and Kevin McCoy, *N.Y. Foundation Linked To Iran’s Islamic Militants*, *Newsday*, republished by *Seattle Times* (May 26, 1995), 1995 WLNR 1308563. The same *Newsday* report also disclosed that “[the Bonyad Mostazafan]’s secretary until 1992, Mojtaba Hesami-Kiche, was at the same time the executive secretary of Vena Industries, a German company wholly owned by [the Bonyad Mostazafan], according to public records filed in Germany. U.S. sources said that Vena has been active in “military procurement” for the Tehran regime.” *Id.*

501. When *Newsday* published its investigation revealing that the Bonyad Mostazafan served as a front for providing money, weapons, and logistical support to Hezbollah, the latter was already a U.S.-government designated terrorist group, having been designated by the United States as a Specially Designated Terrorist several months prior. As a result, from 1995 onwards, the Bonyad Mostazafan’s status as a front for Iranian terrorist operations, including the IRGC’s, including the Qods Force’s, support for Hezbollah was widely known in the international business community and known to Defendants.¹⁷³

502. In 1998, *Newsday* again reported on the western intelligence services’ consensus that the Bonyad Mostazafan was a front for funneling funds and weapons to Iranian proxies:

[T]he quasi-official Mostazafan Foundation [] controls billions of dollars of investments in Iran and around the world. The foundation ... **has been accused by western intelligence services of espionage, supporting terrorism** and smuggling arms. ... *Newsday* disclosed in 1995 that several officers and directors ... had been implicated in arms and technology shipments to Iran, that it was controlled by Iran’s clerical leadership and that the **FBI believed it had served as a front for**

¹⁷³ For example, the *American Spectator* published an expose in 1995 that revealed multiple Bonyad Mostazafan uses of the U.S. banking system to route funds to terrorist operatives and fronts, and the presence of an IRGC-controlled bank in its New York offices. See Kenneth R. Timmerman, *Islamic Iran’s American Base*, *American Spectator* (Dec. 15, 1995) (discussing the IRGC’s use of the Alavi, i.e., the Bonyad Mostazafan, to support terrorist operatives).

*placement in the United States of Revolutionary Guards [Qods Force], Iranian zealots who conducted espionage and stole military technology.*¹⁷⁴

503. After these two *Newsday* reports in 1995 and 1998, the media regularly published similar reports thereafter, which routinely described the Bonyad Mostazafan as a front or funding source for Iranian-backed terrorists operating in the Middle East, including Hezbollah.

504. On December 17, 2008, the U.S. government reinforced its messaging that the Bonyad Mostazafan was a terrorist front that served to raise money and source weapons for Hezbollah, the Qods Force, and Regular IRGC. On that date, the U.S. Departments of Justice, Treasury, and State all announced enforcement actions and sanctions against the Bonyad Mostazafan, and the U.S. Department of State's Counterterrorism Office issued a press release calling attention to U.S. sanctions against entities affiliated with Bonyad Mostazafan.

505. The heightened U.S. crackdown on the Bonyad Mostazafan caused a new round of media coverage drawing attention to the Bonyad Mostazafan's status as a front for Iranian terror. For example, the *Washington Post* reported that:

A Fifth Avenue building ... is secretly co-owned by an Iranian bank that helped finance that country's nuclear program, the Justice Department alleged []. Justice is seeking to seize the share of the property ..., charging that 40 percent of [the building] was actually co-owned by Iran's Bank Melli ...[,] [which] was previously designated by the Treasury Department as a key financier of ... the **[IRGC] and the Quds Force, which has been linked to terrorist groups.** ... "This **scheme to use a front company ... to funnel money from the United States to Iran is yet another example of Iran's duplicity,**" said Stuart Levey, the Treasury Department's undersecretary for terrorism and financial intelligence.¹⁷⁵

¹⁷⁴ Knut Royce, *No Legal Recourse In Iranian's Case / Supreme Court Won't Reopen Suit*, *Newsday* (Dec. 8, 1998), 1998 WLNR 604387 (emphasis added). Regular IRGC agents placed in the U.S. through the Mostazafan Foundation were acting outside Iran and thus Qods Force.

¹⁷⁵ Glenn Kessler, *U.S. Links Iranian Bank To Fifth Avenue Building*, *Washington Post* (Dec. 18, 2008) (emphases added), 2008 WLNR 28032529.

506. The Bonyad Mostazafan’s notorious reputation for directly funding Iranian terrorist proxies in the Middle East continued at all relevant times. For example, in 2014, Jonathan Schanzer, the Vice President of Research at the Foundation for Defense of Democracies, testified that “[t]he Bonyad-e Mostazafan” was “a splinter of Iran’s IRGC” and had “reportedly opened its coffers to Hamas, providing critical financial support.”¹⁷⁶

507. On November 18, 2020, the U.S. Treasury Department designated the Bonyad Mostazafan, observed that it served as a “bridge to the IRGC,” and announced as follows:

Treasury’s Office of Foreign Assets Control (OFAC) took action today against a key patronage network for the Supreme Leader of Iran, the Islamic Revolution Mostazafan Foundation (Bonyad Mostazafan, or the Foundation) ... While Bonyad Mostazafan is *ostensibly* a charitable organization charged ..., its holdings are expropriated from the Iranian people and are used by [Ayatollah] Khamenei to ... enrich his office, reward his political allies, and persecute the regime’s enemies. ... “Iran’s Supreme Leader uses Bonyad Mostazafan to reward his allies under the *pretense of charity*,” said Secretary Steven T. Mnuchin. ...

PARVIZ FATTAH, BONYAD MOSTAZAFAN’S BRIDGE TO THE IRGC
Bonyad Mostazafan maintains close ties to the IRGC, personified by current Foundation president and former IRGC officer **Parviz Fattah**. Appointed to the presidency of the Foundation by the Supreme Leader in July 2019, Fattah previously served as head of the Imam Khomeini Relief Committee, whose Lebanon branch was designated pursuant to *counterterrorism authorities in 2010 for being owned or controlled by, and for providing financial and material support to, Hizballah*. Known for his loyalty to the Supreme Leader, Fattah has also forged ties to senior IRGC-Qods Force (IRGC-QF) officials. According to Fattah, former IRGC-QF commander Qassem Soleimani sought Fattah’s assistance to finance the Fatemiyoun Brigade, an IRGC-QF-led militia composed of Afghan migrants and refugees in Iran coerced to fight in Syria under threat of arrest or deportation. . . . The Fatemiyoun Brigade, like the IRGC-QF itself, is designated pursuant to [] counterterrorism ... authorities. ...

SANCTIONS IMPLICATIONS

As a result of today’s action, ... OFAC’s regulations generally prohibit all dealings by U.S. persons or within (or transiting) the United States that involve

¹⁷⁶ Statement of Jonathan Schanzer, Vice President of Research at the Foundation for Defense of Democracies, Committee on House Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade. Subcommittee on the Middle East and North Africa, *Hamas and Terrorism*, Congressional Testimony via FDCH (Sept. 9, 2014), 2014 WLNR 24926764.

any property or interests in property of blocked or designated persons. In addition, persons that engage in certain transactions with the individuals or entities designated today may themselves be exposed to sanctions. ...

U.S. Treasury Dep't, *Treasury Targets Vast Supreme Leader Patronage Network and Iran's Minister of Intelligence* (Nov. 18, 2020) (emphases added).

508. The Bonyad Mostazafan primarily serves as a front for terror and performs little legitimate charitable work. As the Treasury Department found when it imposed sanctions, “[w]hile the Supreme Leader enriches himself and his allies, the Foundation’s primary mission to care for the poor has *become a secondary objective*. According to the Foundation’s previous president, in past years as little as *seven percent of the Foundation’s profit* has been spent on projects aimed at reducing poverty.” *Id.* (emphases added).

509. The Bonyad Mostazafan directly funds Iranian terrorist proxy military activities outside of Iran. Fattah, who currently runs the Bonyad Mostazafan, has publicly admitted it.

510. Fattah was separately designated for his terrorism-related connections in 2010. U.S. Treasury Dep't, *Fact Sheet: Treasury Designates Iranian Entities Tied to the IRGC and IRISL* (Dec. 21, 2010) (“Parviz Fattah, the Executive Director of Bonyad Taavon Sepah was designated today for acting on behalf of, and providing services to, Bonyad Taavon Sepah.”).

511. The Bonyad Mostazafan’s participation in Irancell played persuaded the State Department to conclude (as published online) that Irancell was “fully owned by the IRGC.”

B. Iran Electronics Industries

512. Iran Electronics Industries, also known as IEI, Sanaye Electronic Iran, Sasad Iran Electronics Industries, or Sherkat Sanayeh Electronics Iran (“IEI”), was and is a front for Hezbollah, the Qods Force, and Regular IRGC.

513. IEI’s express purpose was and is to raise funds and obtain weapons (including weapons components) for the benefit of the IRGC’s, including the Qods Force’s, terrorist

operatives and proxies, including Hezbollah. Funds and weapons (including weapons components) obtained by IEI through its commercial transactions inevitably flowed through IEI to Hezbollah and the Qods Force and, through them, to al-Qaeda and the Taliban, to fund and arm al-Qaeda and Taliban attacks against Americans in Afghanistan from 2007 through the present.

514. Since the 1990s, IEI has been widely known in business, diplomatic, military, and media circles to be an IRGC front for Hezbollah, the Qods Force, and Regular IRGC terror.

515. In 2006, U.S. Treasury official Stuart Levin told agents of MTN's competitor, Turkcell, that IEI was "fully owned" by Hezbollah, the Qods Force, and Regular IRGC.

516. On information and belief, Undersecretary Levey communicated to MTN Group that IEI was "fully owned" by the IRGC and that economic interactions with IEI foreseeably aided Iranian proxy terrorist attacks against Americans.

517. On September 17, 2008, the U.S. Treasury Department designated IEI and explained that it builds weapons intended for use against the U.S. military.¹⁷⁷

518. IEI's participation in Irancell played a role in persuading the State Department to conclude (as published online) that Irancell was "fully owned by the IRGC."

C. MTN Irancell

519. MTN Irancell is a joint venture between two IRGC, including Hezbollah and the Qods Force, fronts, the Bonyad Mostazafan and IEI, which collectively own 51% of MTN Irancell, and MTN Group Ltd., which owns 49% of MTN Irancell ("MTN Irancell").

520. MTN Irancell was and is a front for Hezbollah, Qods Force, and Regular IRGC.

¹⁷⁷ U.S. Treasury Dep't, *Treasury Designates Iranian Military Firms* (Sept. 17, 2008).

521. MTN Irancell’s express purpose was and is to raise funds and obtain weapons (including weapons components) for the benefit of the IRGC’s, including Hezbollah’s and the Qods Force’s, terrorist operatives and proxies like al-Qaeda and the Taliban. Funds and weapons (including weapons components) obtained by MTN Irancell through its commercial transactions inevitably flowed through MTN Irancell to Hezbollah and the Qods Force and, through them, to al-Qaeda and the Taliban, to fund and arm al-Qaeda and Taliban attacks against Americans in Afghanistan from 2007 through the present.

522. The U.S. State Department purportedly referred to Irancell (as published online) as being “fully owned by the IRGC.”

523. Irancell’s recognized status as being “fully owned by the IRGC” was also widely reported in the media, beginning in 2010 with the initial *WikiLeaks* reporting, and continuing thereafter. For example, in 2012, the news commentator Greta Van Susteren noted on her widely-watched Fox News show: “we’re talking about Iran, which is trying to wipe ... Israel off the map, ... and **this joint venture** with [MTN Irancell], **it was not a mystery**. In fact, the [U]ndersecretary of [the Treasury, Stuart Levin in] 2006 according to [] *WikiLeaks* ... said that the Iran Cell was [] **fully owned by the Iranian Revolutionary Guard** [Corps].”¹⁷⁸

524. IRGC specialists agree. For example, in 2015, Dr. Emanuele Ottolenghi, of the Foundation for Defense of Democracies, identified “telecommunications” as a “sector where the IRGC [was] bound to reap economic benefits” because “all three mobile operators in Iran” –

¹⁷⁸ FOX: On the Record, *Interview with Byron York* (August 7, 2012), 2012 WLNR 16563491 (emphasis added).

including MTN Irancell – “are directly or indirectly partners with IRGC-affiliated companies.”¹⁷⁹

D. Telecommunications Company Of Iran (TCI)

525. The Telecommunications Company of Iran (or TCI) was and is a front for Hezbollah, the Qods Force, and Regular IRGC.

526. TCI is the parent company of MTN Irancell’s nominal competitor in Iran, MCI.

527. TCI’s express purpose was and is to raise funds and obtain weapons (including weapons components) for the benefit of Iran’s terrorist operatives and proxies, including Hezbollah.¹⁸⁰ Funds and weapons (including weapons components) obtained by TCI through its commercial transactions inevitably flowed through TCI to Hezbollah and the Qods Force and, through them, to al-Qaeda and the Taliban, to fund and arm al-Qaeda and Taliban attacks against Americans in Afghanistan from 2007 through the present.

528. TCI is known to be an IRGC, including Hezbollah and the Qods Force, front. The *Economist*’s due diligence unit, the *Economist Intelligence Unit*, reported in 2009 that “[t]he question of possible IRGC involvement in the TCI acquisition was raised in subsequent discussion in the Iranian majlis (parliament),” where “[t]he speaker, Ali Larijani, [was] quoted by ... an Iranian newspaper[] as saying that the IRGC was a direct party to the deal.”¹⁸¹ The

¹⁷⁹ Statement of Dr. Emanuele Ottolenghi Senior Fellow Foundation for Defense of Democracies, Committee on House Foreign Affairs Subcommittee on Middle East and North Africa, *Iran Nuclear Deal*, Congressional Testimony via FDCH (Sept. 17, 2015), 2015 WLNR 27612447 (“Dr. Ottolenghi Sept. 17, 2015 Testimony”).

¹⁸⁰ For example, media outlets reported, based on purported U.S. cables published online, TCI built Hezbollah's secure fiber optic network in Lebanon. *E.g.*, Guardian, *Lebanon Told Allies of Hezbollah's Secret Network, WikiLeaks Shows* (Dec. 5, 2010), <https://tinyurl.com/2p8by4k3>.

¹⁸¹ Economist Intelligence Unit, *Iran Telecoms: Dial I for IRGC?*, Telecoms and Technology Forecast (Oct. 12, 2009), 2009 WLNR 20135393.

same report also noted the “[b]lurred distinctions” between the IRGC and Iranian telecom companies:

[In 2006,] Ayatollah Ali Khamenei[] lent his personal support to the proposed asset sales. As with many other privatisation programmes in authoritarian states, there are strong grounds to suspect that elite groups are manipulating the process to advance their own interests unfairly. It is clear that over the past few years much political and economic power has flowed towards the IRGC. ... The telecoms sector in Iran has expanded rapidly over the past five years, in particular in the mobile segment, which recorded a compound annual growth rate of 65% between 2003 and 2008. There is still room for expansion of mobile telephony as the penetration rate is only about 70%, and broadband services are notably underdeveloped. ***This makes telecoms one of the most attractive targets for investment in Iran.*** At the same time, telecoms is a critical sector for the security forces, as the Islamic Republic faces unprecedented domestic opposition along with growing external threats. ***If the IRGC is indeed behind the TCI deal, it would make sense from both the commercial and the security perspective.***¹⁸²

529. Other media reports also alerted Defendants that TCI was a known IRGC front.¹⁸³

530. IRGC specialists concur. For example, when Dr. Ottolenghi identified “telecommunications” as “[a]nother sector where the IRGC [was] bound to reap economic benefits,” Ottolenghi also noted that “[t]he IRGC control[led] Iran’s largest telecom company, the Telecommunication Company of Iran or TCI,” which the “[t]he Guards bought ... in

¹⁸² *Id.* (emphasis added).

¹⁸³ See, e.g., BBC Int’l Reports, *Iranian News Media, Websites Targeted In Wake Of Protests* (Dec. 29, 2009) (noting that Iran’s “main ISPs depend on the Telecommunication Company of Iran (TCI), a company that was bought by the Revolutionary Guards in September”); Christian Science Monitor, *Iran’s Revolutionary Guard Tightens Grip* (Dec. 6, 2009) (the IRGC “bought a 50 percent, \$7.8 billion stake in Iran’s newly privatized telecommunications company”); Newsweek U.S. ed., *Iran’s Dirty Hands* (Nov. 30, 2009) (noting the “shady transaction” in which “the Telecommunication Co. of Iran, ... was essentially handed over to the Revolutionary Guards”); Guardian, *Revolutionary Guards Buy 51% Stake in Iran’s Telecommunications Company* (Oct. 7, 2009) (“Iran’s Revolutionary Guards have bought a controlling stake in the country’s telecommunications company, fuelling suspicions that the organisation is quietly staging a military takeover.”).

September 2009 in a controversial bid that at the last minute disqualified the only non-IRGC offer.”¹⁸⁴ As Dr. Ottolenghi further explained:

TCI’s main shareholder is now Toseye Etemad Mobin (50%), a company ***controlled by the IRGC*** jointly with the supreme leader’s financial network, through two companies - the Tadbir Group-owned Gostaresh Electronic Mobin and Shahriar Mahestan Company. TCI has a monopoly over Iran’s landlines, and thus controls much of the country’s Internet traffic. As *Al-Monitor* reported in August 2013, ***all three mobile operators in Iran are directly or indirectly partners with IRGC-affiliated companies.***¹⁸⁵

E. The Akbari Front Companies

531. Mahmood Akbari, also known as John Wasserman (herein, “Akbari”), was an Iranian national who purchased dual-use commercial grade computers, related equipment and services from illegal sources in the United States to benefit Hezbollah, the Qods Force, and Regular IRGC. On information and belief, Akbari was an IRGC operative who was used by the Qods Force to serve as a cut-out to help source dual-use technology from America for use by IRGC Syndicate Terrorist Proxies to attack Americans in Afghanistan, doing so upon the instruction of one or more Defendants.

532. Patco Group Ltd. (“Patco”) was a company in the U.A.E. operated by Akbari for the purpose of receiving commercial grade computers and related equipment from illegal sources in the United States to benefit Hezbollah, the Qods Force, and Regular IRGC.

533. Managed Systems and Services (FZC) (“MSAS”) was a company in the U.A.E. operated by Akbari and used as a front company and consignee for computer parts to make it appear that the computer parts were being sent to the U.A.E. when in fact they were being diverted to Iran.

¹⁸⁴ Dr. Ottolenghi Sept. 17, 2015 Testimony.

¹⁸⁵ *Id.* (emphasis added).

534. TGO General Trading LLC, also known as Three Green Orbit (herein, “TGO”), was a company in the U.A.E. operated by Akbari and used as a front company to make it appear that payments were being made from the U.A.E., rather than from Iran.

535. On information and belief, Patco, MSAS, and TGO (collectively, “Akbari Entities”) were fronts for Hezbollah, the Qods Force, and Regular IRGC that served as cut-outs in order to help Hezbollah, the Qods Force, and Regular IRGC source sensitive dual-use technology from America for the benefit of Iran’s terrorist operatives and proxies, including Hezbollah. Funds and weapons (including weapons components) obtained by the Akbari Entities through their commercial transactions inevitably flowed through Akbari Entities to Hezbollah, the Qods Force, and Regular IRGC, and through them, to IRGC proxies including, among others, al-Qaeda and the Taliban, to fund and arm the Syndicate terrorist attacks against Americans in Afghanistan from 2012 through 2017.

F. Exit40

536. Exit40 was a front for Hezbollah and the Qods Force.

537. Exit40 procured funds and sensitive dual-use technology from America for the benefit of the IRGC’s terrorist enterprise, including the campaigns of IRGC proxies like al-Qaeda and the Taliban.

538. Funds and weapons (including weapons components) obtained by Exit40 through their commercial transactions with Defendants inevitably flowed through Exit40 to Hezbollah and the Qods Force and, through them, to al-Qaeda and the Taliban to fund and arm al-Qaeda’s and the Taliban’s terrorist attacks against Americans in Afghanistan from 2011 through 2016.

VI. EACH DEFENDANT ENGAGED IN COMMERCIAL TRANSACTIONS THAT IT KNEW WERE STRUCTURED TO FINANCE, ARM, LOGISTICALLY AID, AND/OR OPERATIONALLY SUPPORT HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, AND THEIR TERRORIST PROXIES IN AFGHANISTAN

F. The MTN Defendants

1. MTN Group Joined The Conspiracy To Seize The “Virgin” Telecom Markets Controlled, Contested, Or Influenced By The IRGC And Its Terrorist Proxies

539. The MTN Defendants consist of two companies that each provided material support to Hezbollah, the Qods Force, the Regular IRGC, and the Taliban (MTN Group and MTN Dubai) and one company that served as a front for the IRGC (MTN Irancell). MTN Group and MTN Dubai held themselves out as responsible for how MTN Group affiliates worldwide manage “security” issues, including MTN Afghanistan.

540. MTN Group joined the Conspiracy to enable MTN to seize the “virgin” telecoms markets that dominated the Middle East from 2003 through 2021, including the markets of Iran, Afghanistan, Syria, Lebanon, and Yemen, all of which were controlled, contested, or influenced by the IRGC and/or the IRGC’s terrorist proxies.

541. MTN Group oversaw and authorized MTN Afghanistan’s practice of providing support to the Taliban, as well as MTN Group’s and MTN Dubai’s aid routed through MTN Irancell, Exit40, and the other sources of MTN Irancell-related cash-flow alleged herein.

542. MTN Group executed the Letter Agreement with the Iranian Shareholders on behalf of the entire MTN corporate family. On information and belief, the President of MTN Group was personally compelled to do so during an in-person meeting at the Bonyad Mostazafan office in Tehran, Iran, when an IRGC Regular Brigadier General communicated to MTN Group’s President that the Iranian Shareholders insisted that MTN Group execute the Letter Agreement on behalf of the entire MTN corporate family.

543. On information and belief, the Letter Agreement reflects the Iranian Shareholders' template "Security Aid" agreement, and the Iranian Shareholders specifically styled MTN Group as "MTN" in the Letter Agreement to reinforce to MTN Group and its President, that he was committing the entire MTN corporate family to the deal.

544. It would not be proper to interpret the reference to MTN Group's performance of its "security" related services for the Iranian Shareholders to be limited to being "in South Africa." That passage was a reference by the Iranian Shareholders to their prior frustration with Turkcell, whose C-Suite leadership, on information and belief, refused to commit to providing "security" services to the Iranian Shareholders.

545. MTN Group maintained direct contact with the MTN Afghanistan security official responsible for interfacing with the Taliban, and MTN Group officials encouraged and approved MTN Afghanistan's practice of paying off the Taliban. MTN Group also instructed MTN Afghanistan to comply with the Taliban's directives to switch off its cell towers at night.

546. MTN Group also furthered the Conspiracy by coordinating strategic communications to provide concealment for the Conspiracy by reaching into the United States to communicate IRGC disinformation concerning whether Irancell is an IRGC front.

547. MTN Group and MTN Dubai worked closely to coordinate the technical buildout of MTN Irancell, and senior executives from MTN Group and MTN Dubai regularly coordinated their financial, technical, and logistical support to MTN Irancell.

548. Plaintiffs use the term "MTN" in this section to refer collectively to the MTN family of companies. Unless otherwise specified, when Plaintiffs use that term to describe MTN's conduct in Afghanistan, "MTN" refers to on-the-ground conduct by MTN Afghanistan and approved by both MTN Group and MTN Dubai, and when Plaintiffs use that term to

describe MTN's conduct concerning Irancell and outside of Afghanistan, "MTN" refers to on-the-ground conduct by MTN Irancell and approved by both MTN Group and MTN Dubai.

2. MTN Group, MTN Dubai, And All MTN Subsidiaries And Affiliates Worldwide Joined The Terrorist Conspiracy

549. MTN Group and MTN Dubai joined the Conspiracy more than seventeen (17) years ago in September 2005, when MTN Group's President and CEO executed the IRGC's terrorist template contract on behalf of all MTN entities worldwide. This committed MTN Group, MTN Dubai, and every other MTN entity to provide "security" assistance to the "Iranian Shareholders," meaning Hezbollah, the Qods Force, and Regular IRGC.

550. MTN Group and MTN Dubai have not exited the Conspiracy.

551. Beginning in 2004, MTN Group and MTN Dubai pursued an aggressive expansion in the Middle East, in which MTN Group and MTN Dubai worked together to dominate the "virgin" mobile markets of Iran, Afghanistan, Lebanon, Syria, and Yemen, meaning, a telecommunications market that was substantially undeveloped and required a comprehensive, top-to-bottom, build-out by a multinational telecommunications corporation.

552. By 2004, few "virgin" market opportunities remained in the world. The collective market share attributed to this Iranian-dominated "Shiite Crescent" of Iran, Syria, and Lebanon, combined with the two other nations where Iran actively fomented terrorist proxies (Afghanistan and Yemen), was by far the most lucrative "virgin" mobile phone market opportunity worldwide.

553. MTN Group and MTN Dubai knew that the IRGC, through its subordinate divisions, Hezbollah and the Qods Force, actively sponsored anti-American terrorism in all five of the "virgin" markets they coveted: Iran, Syria, Lebanon, Afghanistan, and Yemen. Mobile phone companies like MTN Group and MTN Dubai are heavily dependent upon infrastructure vulnerable to terrorist attacks. As a result, MTN Group and MTN Dubai knew they would have

to reach an agreement with the IRGC, which was the only way MTN Group and MTN Dubai could win the business, not just in Iran, but also in its client states (e.g., Syria, Lebanon), or where it played a spoiler role (e.g., Afghanistan). This meant MTN Group and MTN Dubai had to make a deal with the IRGC as the latter exercised a de facto veto over the telecoms' procurement decisions in Syria and Lebanon (among other places).

554. In 2004, Iran awarded a cellular-phone license to MTN's competitor, Turkcell. MTN then engaged in a corrupt scheme to take the license away from Turkcell and enter the Iranian market itself. MTN's efforts were successful and led it to acquire a 49% stake in Irancell – a joint venture with an Iranian government-controlled consortium. MTN internally called its corrupt scheme to enter the Iranian market "Project Snooker".¹⁸⁶

555. MTN threw itself into Project Snooker with abandon, dedicating senior MTN Group executives to the mission, including, but not limited to, its President and CEO, Commercial Director, and the regional head responsible for the Middle East.

556. On November 16, 2004, MTN's Commercial Director, Irene Charnley, documented MTN's aggressive support for the terrorist agenda of Hezbollah, the Qods Force, and Regular IRGC. In a fax to Iranians, Ms. Charnley provided MTN's help to Iranian efforts to violate terror-related sanctions against Hezbollah, the Qods Force, and Regular IRGC by sourcing "major components" for American-made "Bell" and "Sikorsky" helicopters that were intended, in part, for "military use" by Hezbollah, the Qods Force, and Regular IRGC.

557. Project Snooker required close cooperation between MTN and the Iranian government. On July 5, 2005, MTN sent a letter from its CEO to two Iranian terrorists, one of

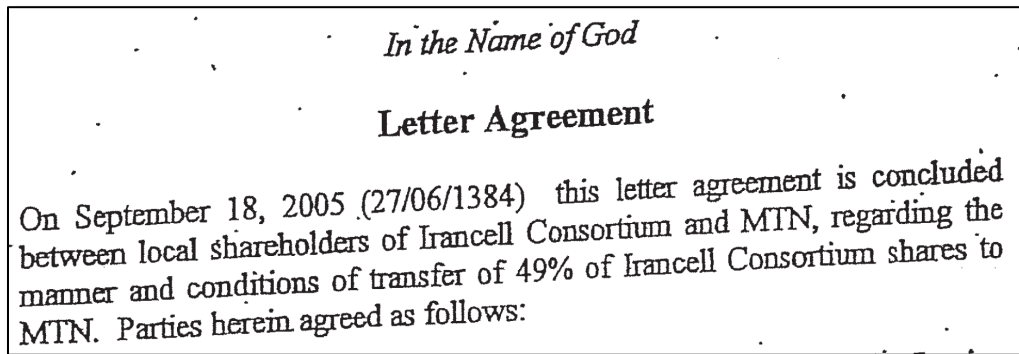
¹⁸⁶ See Memorandum from Phuthuma Nhleko to Sifiso Dabengwa *et al.*, *Overview & Way Forward – Project Snooker* (Sept. 21, 2005) ("*Project Snooker Mem.*").

whom was the former Chief of Staff of the IRGC who had led the Bonyad Mostazafan and IEI, which were the two terrorist fronts with which MTN was attempting to join in the Irancell joint venture (the “July 5, 2005 Letter”). In the July 5, 2005 Letter, MTN Group wrote to its prospective IRGC, including Hezbollah and the Qods Force, joint venture partner, stating that it was “convinced that your organizations together with MTN could create a partnership that would be mutually beneficial in meeting all our objectives in the telecommunications sector in Iran,” and emphasizing “[t]he nature and extent of financial assistance that the MTN Group could provide to the Iranian partners in the Second Mobile licence in Iran” and the “co-operation between your esteemed organizations and the MTN Group in current and future telecommunications projects in Iran.”

558. The negotiations were successful. On September 18, 2005, MTN Group signed a Letter Agreement with the IRGC and Qods Force fronts with whom MTN had been negotiating. It made MTN a junior partner in the MTN Irancell joint venture with a 49% stake, leaving 51%—and all decision-making authority—to MTN’s two partners that MTN knew were IRGC and Qods Force fronts.

559. The Letter Agreement was drafted by the IRGC and constitutes the IRGC’s template for the terms under which Iranian terrorist fronts in industries essential to the terrorist enterprise are permitted to enter business arrangements with foreign companies such as Defendants MTN, ZTE, and Huawei. The Letter Agreement is replete with indicia that it was drafted by the IRGC rather than a sophisticated multinational corporation like any of the Defendants. Such indicia include but are not limited to: (1) the reference to God at the start of the Agreement; (2) the inclusion of the Iranian calendar date (27/06/1384) in the Agreement; (3) the generic reference to “local shareholders” (and later “Iranian Shareholders”) rather than any

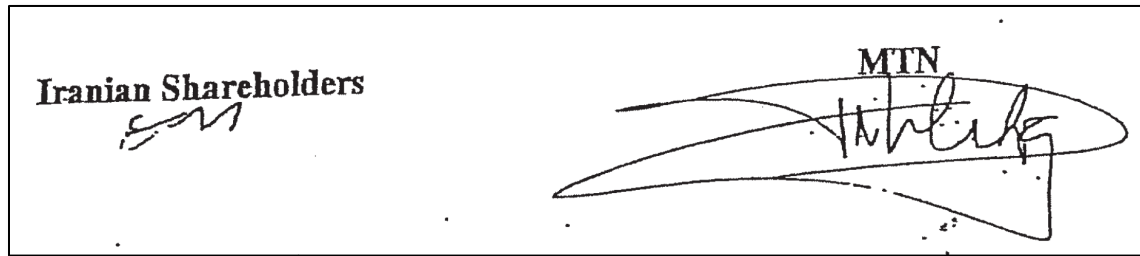
specific reference to any specific Iranian entity; and (4) the inclusion of a blank space for the handwritten insertion of certain terms. Here is how the Agreement begins:



560. MTN secured its joint venture with Hezbollah, the Qods Force, and Regular IRGC — i.e., MTN Irancell — through MTN Group’s direct contractual promise to the IRGC, its Hezbollah Division, and Qods Force. This was done to aid the IRGC and Qods Force terrorist enterprise and MTN’s corrupt payments to one or more IRGC and Qods Force agents. The Letter Agreement pledged broad cooperation between MTN Group and its IRGC, including Hezbollah and the Qods Force, partners in furtherance of Iran’s terrorist agenda. Section 8 obligated MTN Group to assure that, with respect to its new “Iranian shareholder[]” partners, “[t]he cooperation between MTN and Iranian shareholders should be in the line of defensive, security and political cooperation.” Notably, Section 8 expressly contemplated that MTN would work with new IRGC partners outside of Iran: “MTN shall fully support cooperation regarding the aforementioned issues in South Africa.”

561. Thus, MTN officers, employees, and agents directly partnered with Qods Force operatives because when MTN “fully” cooperated on “security” matters with IRGC operatives and agents outside of Iran as it contractually promised to do, MTN was directly aiding Qods Force terrorists because IRGC personnel acting outside of Iran are Qods Force.

562. The Letter Agreement’s deliberately ambiguous references to “Iranian shareholders,” rather than the Iranian entities with which MTN Group was reportedly partnering, was itself an indication of, and evidence that, the Iranian shareholders in MTN Irancell were fronts, operatives, and agents for Hezbollah, the Qods Force, and Regular IRGC. Indeed, the execution of the Agreement was deliberately designed to obscure each signatory:



563. The Letter Agreement did not merely obligate MTN Group to help Hezbollah, the Qods Force, and Regular IRGC source weapons in furtherance of the IRGC’s, including Hezbollah’s and the Qods Force’s, “security” agenda. It also obligated MTN to both pay its new IRGC front partners as well as serve in effect as their financial manager:

- (i) Section 2 required that MTN Group “agree[] to put in trust twenty-one (21) percent of Irancell Consortium before Bank Melli as trustee.” Bank Melli is another front for the IRGC (including Hezbollah and the Qods Force) and has itself been sanctioned by the U.S.
- (ii) Section 3 required that MTN pay Hezbollah, the Qods Force, and Regular IRGC hundreds of millions of dollars in up-front license fees as a condition for becoming the new junior partner in the Irancell joint venture, and that “MTN and Bank Melli shall be responsible for arranging project financing.”
- (iii) Section 7 adds a catch-all provision designed to route additional money from MTN Group to Hezbollah, the Qods Force, and Regular IRGC and provided that: “[t]he costs and expenses incurred by Iranian shareholders” – i.e., Irancell’s two IRGC, including Hezbollah and the Qods Force, fronts – “if any, due to transfer of Irancell’s share to MTN shall be compensated by MTN.” On information and belief, MTN routed millions of additional dollars to Hezbollah, the Qods Force, and Regular IRGC under Section 7.

564. Although MTN was the IRGC’s junior partner in the MTN Irancell joint venture, the Letter Agreement nonetheless empowered MTN with the legal authorities it needed to

effectively shut down the IRGC's, including Hezbollah's and the Qods Force's, ability to weaponize MTN Irancell as an instrument of terror. Most directly, MTN could immediately and unconditionally announce its plans to rapidly exit the joint venture.

565. MTN is also responsible for MTN Irancell's conduct because MTN had (and continues to have) veto power over most of the major decisions at MTN Irancell, similar to the veto possessed by its joint venture partners, the terrorist fronts Bonyad Mostazafan and IEI. For example, Section 5.1 of the Agreement provides that "[t]he resolutions on the below mentioned issues require the affirmative votes of MTN":

- "Annual business plans and budgets of [MTN Irancell], including, but not limited to, medium and long term financing;"
- "Major acquisitions, partnerships, formation of joint ventures or consortiums;"
- "Discontinuation of business activities;"
- "Entering into any agreement with persons, individuals or entities that are directly or indirectly related to Non-Iranian or Iranian Shareholders;"
- "Charging the assets of the Company in any manner which could have significant impact on the Company's ability to use or benefit from its assets in its ordinary course of business;"
- "Profit appropriates and dividend policy; and"
- "Approval of annual accounts." (Ex. A, Letter Agreement, § 5.1.)

566. The Letter Agreement confirmed that MTN promised to provide other "off-the-books" value to the Iranian Shareholders with whom MTN had partnered in MTN Irancell, which was itself another obvious reference to MTN's support for the IRGC's, including Hezbollah's and the Qods Force's, terrorist activities. Section 9 provides, "for this agreement to be effective, it is necessary that the above-mentioned documents and related agreements be signed by MTN as well as to pay license fee and equity as provided in [Section 3 of the

Agreement] within 20 days from the signature of Addendum No. 1 to [sic] license agreement, simultaneously, the parties try to finalize the other relevant operational agreements.”¹⁸⁷

567. MTN Group and its “Iranian shareholder[]” joint venture partners went to great lengths to keep the Letter Agreement a secret. The Letter Agreement was a “close hold” document at MTN Group and was only known to a select group of senior MTN Group executives because MTN understood that it memorialized an obviously illegal scheme between MTN Group and two fronts for Hezbollah, the Qods Force, and Regular IRGC. MTN Group also conspicuously failed to obtain any sign-off from any of MTN’s elite, white-shoe global law firms, none of which would have approved the Letter Agreement.

568. Before MTN Group’s President signed the secret Letter Agreement, a senior official on behalf of the IRGC stated to MTN Group, in sum and substance, that the Letter Agreement was the standard template that the Iranian Shareholders use when a counterparty agrees to assist, among other things, the Iranian Shareholders’ “security” operations.¹⁸⁸

¹⁸⁷ In the secret Letter Agreement, the number “1” in this sentence is handwritten into what was obviously a placeholder.

¹⁸⁸ The secret Letter Agreement was an IRGC template belonging to the Agreement’s “Iranian Shareholders” who signed, i.e., the IRGC. This is so because the IRGC, represented by the “Iranian Shareholders,” and MTN Group, represented by MTN Group CEO, Mr. Nhleko, were the only two signatories to the secret Letter Agreement, the form and content of which indicates its Iranian origins. For example, the template’s Islamic and Iranian calendar references show that the template’s drafter and owner resided and conducted business in a commercial environment and/or regulatory regime in which such Islamic contractual references would be expected—an environment far more likely to be found in the IRGC’s headquarters in Tehran, Iran, than MTN Group’s in Johannesburg, South Africa. *Compare* CIA, *South Africa*, The World Factbook (2022) “86%” of South Africa’s population is “Christian” and “1.9%” is “Muslim”), <https://tinyurl.com/3f72rder>, *with* CIA, *Iran*, The World Factbook (2022) (Islam is Iran’s “official” faith, “99.6%” of Iran’s population are “Muslim,” and “0.3%” are “Zoroastrian, Jewish, and Christian”), <https://tinyurl.com/wb39krfd>. Given those facts, the Letter Agreement was derived from an IRGC template, *not* an MTN Group template, which is the only other logical template source for the Letter. For the avoidance of all doubt, Plaintiffs do not allege that the mere presence of Islamic terms in the Agreement, on its own, suggests a link to terrorism.

569. MTN Group, including its President, knew this statement to be a direct reference to IRGC proxy terrorist attacks targeting Americans around the world.

570. A leaked contemporaneous South African intelligence agency report confirmed MTN Group's 2005 terrorism quid-pro-quo with the IRGC and documented MTN's meetings with a delegation of IRGC operatives—led by the head of Iran's Supreme National Security Council, Hassan Rouhani—one month after MTN Group's September 2005 meeting with senior IRGC terrorists at the Bonyad Mostazafan's Tehran headquarters, in which MTN Group's CEO signed the secret Letter Agreement pledging "security" assistance to the "Iranian shareholders," i.e., the IRGC fronts that controlled Irancell, including the Bonyad Mostazafan.

571. MTN Group deliberately concealed the fact that its President and CEO signed the secret Letter Agreement. On information and belief, MTN Group has never publicly admitted that MTN Group's President and CEO signed the secret Letter Agreement.

572. MTN Group's attempts to conceal the Letter Agreement, and the fact that MTN Group's President and CEO signed the secret Letter Agreement, reflects consciousness of MTN Group's guilt and MTN Group's recognition that its promise to assist the Iranian Shareholder's "security" operations, i.e., anti-American terrorism, was illegal.

573. MTN Group's executives quickly got to work after MTN Group executed the Letter Agreement on September 18, 2005. Three days later, MTN's President and CEO, Phuthuma Nhleko, circulated a memorandum from himself to five senior MTN executives (the "September 18, 2005 Memo"). Captioned "**STRICTLY CONFIDENTIAL**" and headed with the subject "**OVERVIEW AND WAY FORWARD – PROJECT SNOOKER**," it provided:

1. **OPPORTUNITY[:]** Project Snooker still presents *one of the most significant "virgin" mobile opportunities in the world*. ... [N]otwithstanding the significant challenges that lie ahead, [MTN] must continue to pursue this opportunity vigorously.

2. **CURRENT STATUS[;]** *The signing of the various agreements this week [under duress]* was to “book our place at the foot of the mountain – we still need to scale it to get to the peak.” It was a choice between inheriting an advanced arrangement [Turkcell revenue share and various negotiated agreements] or taking the chance that the window of opportunity may close on us whilst we try to reconstruct the deal and arrangements from scratch. We chose the former.
3. **RISK AND REWARD[;]** *Snooker is “no normal country”*. The Ministry of Defense, Government controlled banks and companies, together with Government *essentially control all the commercial activity in the country. Consequently, a conventional mindset, orthodox financial and operational approach to this project is unlikely* to provide us with an outcome that I would feel comfortable to recommend to the board on an investment of over €400 million [license fee and working capital] into Snooker. It is therefore imperative to *think laterally on how we can secure the investment* ... in a manner that allows us to penetrate the market achieving an acceptable IRR [i.e., “internal rate of return,” a measure of investment profitability]. ...
4. **TIMING[;]** The expectation is that the license fee should be paid within weeks and the operation launched commercially within a six month period. ... The implied time scale can only be achieved through a well thought out and coordinated project management structure up ...
5. **PROJECT MANAGEMENT[;]** *Given the size of the market*, limited time to launch and all that has to be reviewed and completed before the MTN Group board ratifies the revised business plan, *a special project structure must be put in place*. ... **5.1.2. Finance Structure, project funding and ancillary loan agreements[.]** The Group CFO should take responsibility for this area, primarily in the following categories:
 - Flow of license fee and working capital
 - Appropriate security arrangements for funding of local partners together with the loan agreements
 - Arranging the project finance ...
6. **PROJECT STEERING COMMITTEE[;]** I will chair a project steering committee that will have the responsibility of meeting regularly to oversee both Phase I and Phase II until the project is passed onto the MD / COO. The Steering Committee shall comprise of: CEO[;] COO[;] CFO[;] CTO[;] Commercial Director[;] Group Executive HR ...
8. **CONCLUSION[;]** *This is one of the most significant opportunities the Group will undertake* and will require teamwork to achieve these objectives. (Emphases added; formatting adjusted.)

574. After MTN's executive team successfully executed Project Snooker, the conservative-dominated and Qods Force-applauding Iranian parliament determined that MTN's operation of Irancell would improve Iran's "security."

575. Project Snooker was successful not only because MTN pledged strategic cooperation with the Iranian government, but also because MTN made corrupt payments to government officials, at least one of which it structured as a sham consultancy payment. On December 11, 2006, MTN Group's CEO instructed MTN Group's CFO in writing on MTN letterhead to "finalise all agreements with the consultants" who had "assisted the Company" in obtaining the Iran deal. The first agreement called for MTN Group to make a \$400,000 payment for the benefit of an Iranian government operative. The payment was effectuated through an MTN Group subsidiary, MTN International (Mauritius) Limited, and sent to a consulting firm owned by the Iranian operative's associate. On April 4, 2007, MTN wired the \$400,000 to the putative "consultant." MTN has never proffered a legitimate explanation for that payment.

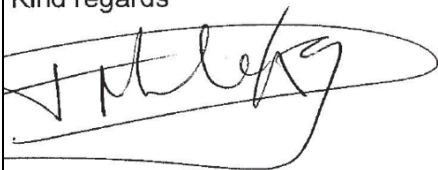
576. MTN's second corrupt payment was to South Africa's ambassador to Iran. MTN's Iran Director has admitted to paying the Ambassador \$200,000 in cash out of his own funds, which he tied to cooperation in helping MTN secure its equity interest in Irancell.

577. MTN Group's senior executives knew of, and approved, MTN Group's bribes to Hezbollah, the Qods Force, and Regular IRGC agents who helped MTN secure the Irancell joint venture. For example, on December 11, 2006, MTN's CEO, Mr. Nhleko, wrote a memorandum (Subject: "**CONSULTANCY AGREEMENTS**") to MTN Group's commercial director, Irene Charnley, in which Mr. Nhleko authorized MTN's bribes (the "December 11, 2006 Memo"):

Dear Irene

With reference to the process in terms of which MTN International (Mauritius) Limited acquired a 49% equity interest in Irancell, you are authorized to finalise all agreements with the consultants that assisted the Company during the run up to and actual negotiating period, and to effect the necessary payments.

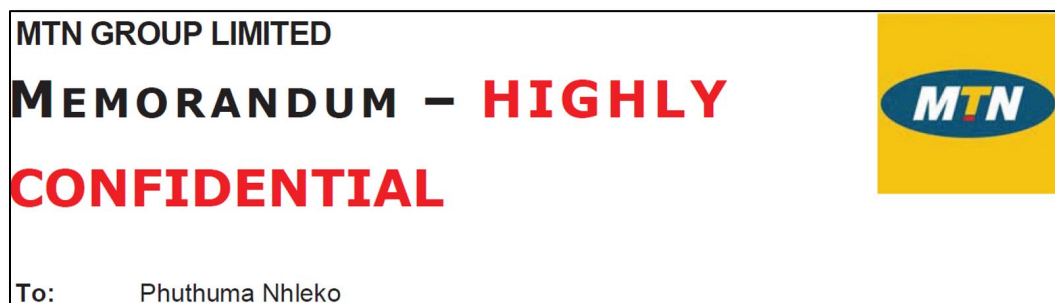
Kind regards



PHUTHUMA F. NHLEKO
GROUP PRESIDENT & CEO

578. The phrase “necessary payments” in the December 11, 2006 Memo was a direct admission that the consultancy payments were bribes. Indeed “necessary payments” has long been understood to refer to bribery.

579. Other internal MTN Group documents, leaked by a whistleblower, also confirm that MTN Group’s executives directed MTN’s financial, technological, and operational aid for MTN Irancell and the IRGC, including Hezbollah and Qods Force, fronts that controlled MTN Irancell. For example, on March 25, 2007, MTN’s regional manager responsible for Iran, Chris Kilowan, sent a memorandum to MTN’s CEO, Mr. Nhleko, which extensively documented MTN Group’s illicit activities and was stamped “HIGHLY CONFIDENTIAL”:



580. In the March 25, 2007 Memo, MTN's regional director responsible for Iran (Mr. Kilowan) confirmed in writing to MTN Group's CEO (Mr. Nhleko), among other things, that:

- (i) Mr. Kilowan understood that "it was the [President of South Africa's] view that the matter of MTN has nothing to do with the Government of South Africa as it is a private business in which the Government of South Africa plays no role."
- (ii) Mr. Kilowan had met with "Mr. Motakki" on behalf of the "Minister of Foreign Affairs" who was, on information and belief, an IRGC, including Qods Force, cut-out who was either relaying a message from the IRGC or acting as an IRGC operative himself.
- (iii) During Mr. Kilowan's meeting with Mr. Motakki, the latter "re-iterated [the IRGC's, Qods Force's] understanding that MTN was allowed to replace Turkcell in exchange for defence co-operation," and that "the office of the Supreme Leader" had directly intervened after Hezbollah, the Qods Force, and Regular IRGC determined "that there [were] significant defence benefits in it for [Hezbollah, the Qods Force, and Regular IRGC] were MTN to be allowed into the process. On that basis [Hezbollah, the Qods Force, and Regular IRGC] withdrew their objections [to a foreign company playing a role in Iran's telecoms sector] and allowed the process to proceed in MTN's favour."
- (iv) Mr. Kilowan understood that MTN Group had only become a candidate for the Irancell joint venture after MTN Group had promised to pledge to aggressively support the "security" needs of Hezbollah, the Qods Force, and Regular IRGC fronts that controlled the Bonyad Mostazafan and IEI. Mr. Kilowan noted, as a "brief recap of history," that "MTN only seriously got back into the [bidding] process" after its Iranian counterparties perceived that MTN would affirmatively aid their "security" needs.

581. Indeed, Mr. Kilowan's March 25, 2007 Memo to MTN Group and Mr. Nhleko underscored to MTN Group that MTN would need to serve as a weapons supplier for its Iranian counterparties, and foreseeably aid Hezbollah, the Qods Forced, and Regular IRGC, if MTN Group wanted to win and maintain MTN's position in the MTN Irancell joint venture:

It would seem clear that the issue of *defence co-operation* has become a pressing matter with the government of Iran. If regard is had to the latest [U.N. Security Council] Resolution there is a clear move towards dealing with Iran's [] weapons ... Russia has traditionally played the *role of key weapons supplier* to Iran. Given recent developments ..., [Russia] is actively looking at more secured suppliers of defence materials. ... Because the entire political situation has now deteriorated significantly it is highly unlikely that the Government of South Africa will be prepared to sign any defence agreements or deliver defence materials to Iran. Given the *clear linkage that the Government of Iran has*

drawn between the defence assistance and allowing MTN into the country the likelihood that there will be serious blowback for MTN is increasing.

Because there has been a recognition of the *non-business imperatives that drove MTN's entry into Iran*, the Distant Thunder ... projects have been developed to deepen MTN's position, as opposed to and distinct from Irancell, inside Iran so that MTN would be able to rely on broad popular support for its continued presence. ... To give MTN a realistic chance to navigate through what is potentially going to be a difficult few months (if not years until the end of the current presidency in 2009), I make the following recommendations:

1. Implementation of Project Distant Thunder at the earliest opportunity. We could pre-empt some of the activity that is almost certain to be started in the public sphere against MTN. ... (Dimension 1)
2. Approval of the creation of the committee to pursue mid to long term strategies for MTN's investment in Iran. (Dimension 2)
3. Finalisation of the diplomatic support initiative. The *first consultant is still waiting for the transfer of the agreed amount. This is causing considerable anxiety in his mind and going forward we are going to need his support.* We still have not given the second consultant any indication whether we are seriously considering his request. He too is developing some anxiety and I have to field almost daily questions on it. (Dimension 3)

582. A November 10, 2007 memorandum from MTN's regional manager responsible for Iran, Chris Kilowan, and MTN's then-CEO, Mr. Nhleko, further documented MTN Group's open support for the illicit activities conducted by the fronts operating on behalf of Hezbollah, the Qods Force, and Regular IRGC with whom MTN had partnered in Irancell, including MTN partners whom MTN nicknamed "Short John" and "Long John" (the "November 10, 2007 Memo"). On information and belief, the Iranian operative whom MTN derisively nicknamed "Short John" was an agent for Hezbollah, the Qods Force, and Regular IRGC.

583. The November 10, 2007 Memo was labeled "**STRICTLY CONFIDENTIAL**" in bright red bolded all-caps font and was titled "**SUBJECT: OUTSTANDING ISSUES**" in bolded all-caps black font. In it, MTN's executive for Iran communicated to MTN's CEO that:

Pursuant to [our] last communication ... I set out below the issues that I believe are still outstanding [] and will have an impact ... on MTN's investment. ...

FINALISATION OF CONTRACT WITH SHORT JOHN[:] Subsequent to our last discussion on this matter [in early 2007] I did not do anything about the agreement, preferring to wait until December [2007] to do an agreement ... I can certainly state that [Short John] has *come to the party on every occasion that I called upon him*. The fact that the *quid pro quo that has threatened at one stage to be the primary stick with which we could be hit has now largely disappeared* because of his efforts. The initial concessions on promised support for the revenue share issue was *because of his direct involvement* ... With me out of the picture he will probably be the only friendly source of information and interaction for MTN on this side. I would recommend that *MTN finalise arrangements with him and offer fair compensation commensurate with the huge role he has played right from the outset*.

RENEWED APPROACH BY LONG JOHN[:] I have communicated this to you a few weeks ago and recently forwarded an SMS from him. The background to this new approach is centered in planned developments within the area that he is currently working. Whatever his motivations, it is not something that should be ignored. While he has very little power to do anything positive, *he can be a destructive force* or simply an unnecessary distraction. ...

PERSISTENT NEGATIVE VIEWS ABOUT SOME MTN EXPATS[:] I beg your forgiveness if I sound like a record with a stuck needle but I ... alert[] you to a serious risk to MTN's investment. ... In [Mr. Mokhber's] view MTN made a mistake and inflicted a huge insult on Iran by placing [a woman] here [as Chief Operating Officer of MTN Irancell]. ... (Bolded all-caps emphases in original; bolded italicized emphases added.)

584. One reason MTN chose to become the joint venture partner of the IRGC, including Hezbollah and the Qods Force, was the potential for enormous profits. As the *Financial Times* reported at the time in 2013, “[a]s the international community was weighing whether to impose yet more sanctions on Iran over its nuclear programme, [MTN President and CEO] Phuthuma Nhleko was making other plans. Instead of seeing a country with mounting

political problems, Mr Nhleko saw a nation with relatively few mobile phone users. Iran, he reckoned, could quickly add 2.5m-3m new customers for MTN Group.”¹⁸⁹

585. After MTN secured its joint venture with two fronts for the IRGC, MTN’s President and CEO, Phuthuma Nhleko, “laughed off questions about the political risk of doing business with Iran.”¹⁹⁰ As he chuckled in a discussion with investors, he stated “[MTN] hadn’t budgeted for bomb shelters or anything like that.”¹⁹¹ MTN’s CEO’s choice to literally “laugh off” questions about the obviously dire risks associated with MTN’s new joint venture in Iran typifies MTN’s deliberate choice to align itself with anti-American terrorists as the cost of doing business as the IRGC’s junior partner in the MTN Irancell joint venture.

586. MTN continued to pursue Project Snooker even after the U.S. Undersecretary of the Treasury told Turkish officials that Irancell was “fully owned” by Hezbollah, the Qods Force, and Regular IRGC. Undersecretary Levey did so as part of a campaign in which he alerted every major western business and financial partner of Hezbollah, the Qods Force, and Regular IRGC about the inherent terrorism risks attendant to any transactions with fronts for Hezbollah, the Qods Force, and Regular IRGC. On information and belief, Undersecretary Levey told MTN Group that Irancell was “fully owned” by Hezbollah, the Qods Force, and Regular IRGC and, by extension, when Irancell operated outside of Iran, Qods Force operatives were in charge.

587. In June 2018, South Africa’s anti-corruption police – called the “Hawks” – raided the offices of MTN and its outside counsel as part of an investigation into Irancell-connected

¹⁸⁹ Lina Saigol and Andrew England, *Telecoms: Dealings in the Danger Zone; MTN of South Africa’s Ventures in Iran and Syria Have Dented Its Reputation and Rattled Shareholders*, Financial Times (July 2, 2013) (“Saigol and England, *Telecoms: Dealings in the Danger Zone*”).

¹⁹⁰ *Id.*

¹⁹¹ *Id.*

bribery. Roughly eight months later, the Hawks also arrested the former Ambassador whom MTN had bribed. On information and belief, that investigation remains ongoing.

588. At bottom, MTN's bribes and alliance with Hezbollah, the Qods Force, and Regular IRGC "is a saga that illustrates the extraordinary risks MTN has taken to profit from doing business with pariah states."¹⁹²

3. MTN Knowingly Assumed A Financial, Logistical, And Operational Role In The IRGC's, Including Hezbollah's And The Qods Force's, Sponsorship And Support Of Terrorist Attacks Against Americans Worldwide

589. For more than seventeen (17) years, MTN Group and MTN Dubai has each served as a reliable joint venture partner for Hezbollah, the Qods Force, and Regular IRGC.

590. MTN Group acted as an international logistics and financial agent for the IRGC, including its Hezbollah Division and Qods Force. In doing so, MTN Group acted within the scope of the instruction from MTN Group (the principal) in the Letter Agreement from the "Iranian Shareholders," committing the MTN Group to assist the "security" operations (i.e., terrorist attacks) of Hezbollah and the Qods Force. Indicia of MTN Group's service as an agent for the IRGC include, but are not limited to:

- (i) MTN Group represented the Iranian Shareholders as their purchasing agent, and coordinated efforts to obtain vital U.S. technology that aided bomb and rocket construction and terrorist surveillance, as requested by IRGC-QF and Hezbollah, reaching into the United States to acquire such gear.
- (ii) MTN Group repeatedly sourced precious U.S. dollars to funnel to IRGC-QF as bribes (\$400,000) or to pay to others as bribes in order to help further conceal IRGC-QF front companies, including pursuing a scheme to bribe the South African UN delegation in order to successfully kill a UN resolution that would have sanctioned IRGC-QF front companies necessary to the terrorist enterprise.
- (iii) MTN Group provided public relations support and crisis management services designed to benefit the IRGC-QF front, MTN Irancell, by coordinating the strategic

¹⁹² *Id.*

communications response to media stories, government investigations, and/or lawsuits that exposed MTN Irancell as an IRGC-QF front, including through actions inside the United States and communications directed towards a specific American audience.

- (iv) MTN Group Organized IRGC-QF finances and managed IRGC-QF assets through Irancell, and MTN Group had to reach into the United States to do so because of the complicated technology that MTN used, which relied on purloined American technology.
- (v) MTN Group coordinated the secret use of U.S. IT experts to handle sensitive tasks that Irancell agents could not, knowing that such persons were working from the United States (indeed that was the point, since MTN needed people with U.S. tech expertise).
- (vi) MTN Group prepared detailed studies at the request of the IRGC-QF that were designed to improve Iranian weapons capabilities, with a specific understanding that the IRGC-QF's primary target was the United States, and therefore that the weapons studies they were sharing would target the United States, including its citizens in the Middle East.

591. MTN Group coordinated with MTN Dubai to manage the procurement scheme.

MTN Group directed the conduct of the purported "third parties" in the U.A.E. who were, in fact, shared corporate covers acting on behalf of both MTN Group, MTN Irancell, and Hezbollah, the Qods Force, and Regular IRGC.

592. MTN Group extracted vast amounts of state-of-the-art American technologies from the U.S. marketplace on behalf of MTN Group's IRGC partners. According to *Reuters'* Special Report, "***MTN [Group] was determined that MTN Irancell procure substantial amounts of U.S. equipment: The U.S. products had performed well in its other networks, and the company's technicians were familiar with them.***"¹⁹³

593. MTN Group, and its employees, set out to evade America's IRGC-related terrorism sanctions. According to *Reuters*, "internal [MTN Group] documents" "show that MTN [Group] employees created presentations for meetings and wrote reports that openly discussed circumventing U.S. sanctions to source American tech equipment for MTN Irancell." *Id.*

¹⁹³ Steve Stecklow, *Special Report: Documents Detail How MTN Funneled U.S. Technology to Iran*, *Reuters* (Aug. 30, 2012).

594. MTN Group’s employees understood that their transaction activities on behalf of the IRGC were illegal. According to *Reuters*, “internal [MTN Group] documents” “show that MTN [Group] employees” “address[ed] the potential consequences of getting caught” in written MTN Group documents. *Id.*

595. MTN Group’s C-Suite directed its support for the Conspiracy, and continued doing so even after MTN Group finished pilfering the Irancell license from Turkcell in 2005:

The new MTN documents appear to detail an *intentional effort to evade sanctions*. For example, a January 2006 PowerPoint presentation prepared for the project steering committee - *comprised of then top-level MTN executives* - includes a slide titled “Measures adopted to comply with/bypass US embargoes.” It discussed how the company had decided to outsource Irancell’s data centre after receiving legal advice. “In the absence of applicable U.S. consents, it is a less risky route to MTN for Irancell to outsource data centre than it is to purchase restricted products,” the PowerPoint slide says. (*Id.*)

596. MTN Group, its executives, and employees, knew there were potential “civil and criminal consequences” to their scheme – and intensified it anyway:

“**CIVIL AND CRIMINAL CONSEQUENCES**” According to [] internal procurement documents, right from the start MTN was well aware of what it termed “embargo issues” and the *inherent risks involved*. A December 2005 PowerPoint presentation marked confidential and emblazoned with MTN’s logo noted that the “*Consequences of non compliance*” included “*Civil and criminal consequences*.” The PowerPoint slide added that the U.S. government could blacklist MTN, “which could result in all MTN operations being precluded from sourcing products/services from U.S. based companies.” (*Id.*)

597. MTN Group, its C-Suite, and its employees had actual knowledge of the scheme. MTN Group personnel routinely prepared written materials that memorialized the illicit importation of embargoed U.S. technologies, for the specific purpose of flowing the technology through to Iran, where MTN Group and its personnel knew there would be only one end recipient: Hezbollah, the Qods Force, and Regular IRGC. Per *Reuters*:

A delivery schedule also dated June 2006 lists U.S. equipment needed for “value-added services,” including voice mail and a wiretapping system. The schedule

states that the equipment would be “Ready to Ship Dubai” that July and August. It estimates it would take two weeks to arrive in the southern Iranian port of Bandar Abbas by “Air or Sea/Road,” and then up to 30 days to clear Iranian customs. According to a person familiar with the matter, the equipment ultimately arrived by boat. “It all showed up,” this person said. (*Id.*)

598. MTN Group maintained “a lengthy spreadsheet of ‘3rd Party’ equipment dated June 2006 that list[ed] hundreds of U.S. components - including servers, routers, storage devices and software - required for a variety of systems.” *Id.*

599. From the course of negotiations with its IRGC, including Qods Force, counterparts in 2004 and 2005, MTN knew at all times that it was acting to benefit the IRGC’s, including Hezbollah’s and the Qods Force’s terrorist agenda. MTN contractually agreed to benefit the “security” needs of its Iranian Shareholders (a direct reference to the two fronts for Hezbollah, the Qods Force, and Regular IRGC with whom MTN agreed to serve as the junior partner in their shared joint venture).

600. MTN Group and MTN Dubai knew that MTN’s pledge to aid the IRGC’s, including Hezbollah’s and the Qods Force’s, “security”-related efforts committed MTN Group and MTN Dubai to actively participating in the IRGC’s, including Hezbollah’s and the Qods Force’s, terrorist enterprise against Americans outside of Iran, including in Afghanistan.

601. MTN Group remained committed to its IRGC, including Hezbollah and the Qods Force, allies even after withering U.S. pressure. For example, in or around 2010 or 2011, MTN representatives met with senior executive officials from the U.S. government. During these meetings, MTN representatives falsely assured the U.S. government that they were not helping Hezbollah, the Qods Force, and Regular IRGC or supplying them with any embargoed U.S. technology in violation of U.S. sanctions against Iran that are intended to deprive Hezbollah, the Qods Force, and Regular IRGC of the money and technology useful to their propagation of

violence against Americans in the Middle East and Afghanistan. MTN provided the U.S. such false assurances even after “MTN ha[d] carried out orders from the regime to shut off text messaging and Skype during times of political protest, and reportedly ha[d] a floor in its Tehran headquarters controlled by Iranian security officials.”

602. Under the structure of the MTN Irancell joint venture, the two fronts for Hezbollah, the Qods Force, and Regular IRGC that exercised 51% control of MTN Irancell – the Bonyad Mostazafan and IEI – had the mandate to promote the IRGC’s, including Hezbollah’s and the Qods Force’s, “security” agenda, including the obligation to block any significant MTN Irancell-related transaction or commercial relationship unless it improved the IRGC’s, including Hezbollah’s and the Qods Force’s, terrorism capabilities. Given the IRGC’s, including the Qods Force’s, view that MTN Irancell was essential to IRGC, including Hezbollah and the Qods Force, “security” operations, the terrorist fronts that controlled MTN Irancell (Bonyad Mostazafan and IEI) would not have approved any material MTN Irancell transaction unless they determined that, on balance, the particular transaction improved the IRGC’s, including Hezbollah’s and the Qods Force’s, ability to execute terror operations as the central element of the IRGC’s “security” agenda. As a result, one may infer that every significant commercial transaction and business relationship that MTN Irancell entered into was: (1) vetted by Hezbollah, the Qods Force, and Regular IRGC; and (2) determined by such terrorists to advance the IRGC’s, including Hezbollah’s and the Qods Force’s, “security”-related capabilities, which was a specific Iranian euphemism for external terror operations.

603. MTN was the lead target of a major public pressure campaign demanding that MTN exit its joint venture with Hezbollah, the Qods Force, and Regular IRGC. For example, on March 7, 2012, UANI “renewed its call on investors, affiliated institutions and potential

customers to cease all business with South African telecommunications firm MTN in response to MTN Group President and CEO Sifiso Dabengwa's callous remarks and irresponsible posture on MTN's partnership with sanctioned Iranian entities that are linked to the Islamic Revolutionary Guards Corps (IRGC)."¹⁹⁴ MTN chose to stay in their alliance with Hezbollah, the Qods Force, and Regular IRGC even after nearly every other multinational had exited such ventures.

604. From 2005 through the present, MTN's joint venture with MTN Irancell, and MTN's illicit transactions with MTN Irancell, the Bonyad Mostazafan, IEI, TCI, the Akbari Fronts, and Exit40 each provided tens of millions of dollars annually in illicit funds, weapons, and operational support to Hezbollah, the Qods Force, and Regular IRGC, which flowed through to al-Qaeda and the Taliban and facilitated attacks against Americans in Afghanistan, including Plaintiffs and their loved ones.

605. **MTN Assumed a Financial Role in the Terrorist Enterprise.** MTN assumed a financial role in the terrorist enterprise by, among other things, bribing its IRGC, including Qods Force, joint venture partners to win the Irancell license in the first instance, paying large license fees, and generating revenue for MTN Irancell throughout the operation of the joint venture.

606. **MTN's Bribes to Terrorist Fronts.** "In Iran, MTN has been accused of paying bribes to South African and Iranian officials to secure a licence there in 2005."¹⁹⁵

607. The recipient of MTN's \$400,000 wire acted as a front, operative, or agent for Hezbollah, the Qods Force, and Regular IRGC. On information and belief, the recipient of

¹⁹⁴ United Against Nuclear Iran ("UANI"), *UANI Responds to MTN CEO's Irresponsible Position on Iran and Renews Call for MTN to End its Business in Iran* (Mar. 7, 2012); see Bus. Wire, *UANI Responds to MTN CEO's Irresponsible Position on Iran and Renews Call for MTN to End its Business in Iran* (Mar. 7, 2012) (broad global publication of UANI press release).

¹⁹⁵ Agence France Presse English Wire, *South African Telecom MTN Gains Clients Despite Scandals* (Mar. 7, 2019).

MTN's \$400,000 wire was a cut-out for MTN to route value to "Iranian shareholders" who were Hezbollah, the Qods Force, and Regular IRGC. Hezbollah, the Qods Force, and Regular IRGC ensures that all economic value is shared amongst constituent parts of the organization, and would not have permitted such value transfer here relating to a contract decision-making process Hezbollah, the Qods Force, and Regular IRGC controlled without obtaining their share of the payment under the IRGC's mafia-like revenue sharing practices.

608. MTN knew, or recklessly disregarded, that the recipient of MTN's \$400,000 wire was acting as a cut-out to allow money to flow through to aid Hezbollah, the Qods Force, and Regular IRGC, which was vital to MTN's successful campaign to steal Turkcell's license.

609. MTN also knew, or recklessly disregarded, that the recipient of MTN's \$400,000 wire instructed MTN to wire the money, in U.S. Dollars, to a bank account in the U.A.E., and therefore that the recipient of MTN's \$400,000 wire was specifically acting as a pass-through for the benefit of the Qods Force because MTN's \$400,000 wire instruction, on information and belief, caused a bank in the United States to send \$400,000 to a bank account controlled by a cut-out for Hezbollah, the Qods Force, and Regular IRGC acting in Dubai, which was the Qods Force's most notorious financial and logistical hub in the Middle East outside of Iran.

610. On information and belief, MTN regularly makes similar sham "consulting" payments like one that MTN used to attempt to justify MTN's \$400,000 wire. Such payments benefitted fronts, operatives, or agents for Hezbollah, the Qods Force, and Regular IRGC in their MTN Irancell-related terrorist fundraising efforts from 2005 through today.

611. **MTN's License Fee Payments to Terrorist Fronts.** After it corruptly secured the 15-year Irancell license, MTN Group Ltd. paid Hezbollah, the Qods Force, and Regular IRGC through the Bonyad Mostazafan and IEI, an approximately \$300 million license fee when

it secured its 49% status as the junior partner in the MTN Irancell joint venture. This money benefited the IRGC's, including Hezbollah's and the Qods Force's, sponsorship of and support for terrorist attacks, and Hezbollah and the Qods Force received a substantial amount per standard practice by the IRGC.

612. **MTN's Funding of Terrorist Fronts through MTN Irancell Cash Flow.** MTN reaped enormous profits from its involvement in MTN Irancell, and sourced copious amounts of dual-use technology to benefit MTN Irancell and Hezbollah, the Qods Force, and Regular IRGC. Indeed, by 2013, "MTN has faced a huge headache in seeking to get dividends out of Iran because stringent sanctions prevent[ed] banks from moving cash easily in and out of the country. MTN ... *was virtually printing money in Iran*, where it has a 46% share of the market."¹⁹⁶

613. Under MTN's joint venture with its two IRGC, including Hezbollah and the Qods Force, front partners in MTN Irancell, for every dollar (or Iranian Rial) MTN generated for the joint venture, MTN's terrorist partners received 51 cents to invest in their terrorist enterprise. Thus, every dollar in profit for MTN Irancell inevitably helped fund Hezbollah's coordination of a nationwide insurgency against Americans in Afghanistan, the IRGC's, including the Qods Force's, industrial-scale production of IED components, advanced rockets, and other high-tech weapons for use by Syndicate terrorists against Americans in Afghanistan led by al-Qaeda and the Taliban, and the aggressive forward deployment of Hezbollah and/or Qods Force operatives inside Afghanistan to facilitate the IRGC's vast storehouse of assistance to the Taliban.

614. Through its participation in MTN Irancell, MTN caused Hezbollah, the Qods Force, and Regular IRGC to realize tens of millions of dollars per year in income that Hezbollah,

¹⁹⁶ Business Day Live, *Iran Deals Forced MTN Boss to Quit* (July 28, 2013) (emphasis added).

the Qods Force, and Regular IRGC used to fund terrorist operations against the U.S. in Afghanistan including, *inter alia*, by funding al-Qaeda and the Taliban.

615. **MTN Assumed an Operational Role in the Terrorist Enterprise.** MTN Group and MTN Dubai deliberately provided “security” assistance to its JV partners, the “Iranian Shareholders,” i.e., Hezbollah, the Qods Force, and Regular IRGC. In its blockbuster Special Report breaking one MTN Group scandal, *Reuters* revealed that “internal documents seen by *Reuters*,” showed that “MTN Group” ***“plotted to procure embargoed U.S. technology products for an Iranian subsidiary through outside vendors*** to circumvent American sanctions on the Islamic Republic.”¹⁹⁷ According to *Reuters*, “[h]undreds of pages of internal documents reviewed by *Reuters* show that MTN employees created presentations for meetings and wrote reports that openly discussed circumventing U.S. sanctions to source American tech equipment for MTN Irancell. ... [and] also address[ed] the potential consequences of getting caught.” *Id.* Indeed, “[t]he documents show that MTN was well aware of the U.S. sanctions, wrestled with how to deal with them and ultimately decided to circumvent them by relying on Middle Eastern firms inside and outside Iran.” *Id.*

616. On August 30, 2012, MTN Group issued a statement to *Reuters*, in which “MTN denied any wrongdoing.” *Id.* According to *Reuters*, “Paul Norman, MTN Group’s chief human resources and corporate affairs officer,” issued a statement to *Reuters*:

MTN denies that it has ever conspired with suppliers to evade applicable U.S. sanctions on Iran or had a policy to do so. MTN works with reputable international suppliers. Our equipment is purchased from turnkey vendors and all our vendors are required to comply with U.S. and E.U. sanctions. We have checked vendor compliance procedures and continue to monitor them and we are confident they are robust. (*Id.*)

¹⁹⁷ Steve Stecklow, *How A Telecom Giant Got Round Sanctions On Iran*, *Reuters* (Aug. 30, 2012).

617. MTN Group's denial was a lie, and MTN Group intended to conceal MTN Group's and MTN Dubai's membership in the IRGC Conspiracy, which MTN Group joined on behalf of itself and MTN Dubai in 2005. MTN Group's statement aided the IRGC's terrorist finance and logistics scheme by engaging in strategic communications targeted at the United States, which maintained MTN Group's status as a viable "cover" for the illicit fundraising and acquisition of embargoed American technologies by Hezbollah, the Qods Force, and Regular IRGC while MTN Group was under scrutiny.

618. As the IRGC's chief outside telecoms partner, MTN Group helped Hezbollah, the Qods Force, and Regular IRGC grow their technical capabilities, evade U.S. sanctions, and acquire embargoed U.S.-made technology. From 2005 through today, MTN has illegally sourced embargoed dual-use U.S. technology at the request of Hezbollah, the Qods Force, and Regular IRGC in coordination with MTN's Qods Force handlers in the U.A.E., where MTN and Hezbollah, the Qods Force, and Regular IRGC coordinate their technical collaboration. Plaintiffs' belief is based upon, *inter alia*, information and inferences derived from witness statements, internal MTN documents, financial data, and mainstream media investigative reports.

619. For example, on June 4, 2012, *Reuters* reported how MTN Group led efforts to illegally acquire hundreds of dual-use, military-grade embargoed communications, telecom, and computer technologies for Hezbollah, the Qods Force, and Regular IRGC. Steve Stecklow, *Exclusive: Iranian Cell-Phone Carrier Obtained Banned U.S. Tech*, *Reuters* (June 4, 2012).

A fast-growing Iranian mobile-phone network managed to ***obtain sophisticated U.S. computer equipment despite sanctions that prohibit sales of American technology to Iran***, interviews and documents show. MTN Irancell, a joint venture between MTN Group Ltd of South Africa and an Iranian government-controlled consortium, sourced equipment from Sun Microsystems Inc, Hewlett Packard Co and Cisco Systems Inc, the documents and interviews show....

Chris Kilowan, who was MTN's top executive in Iran from 2004 to 2007, said in an interview ... [that] ***MTN's parent company, MTN Group, was directly involved in procuring U.S. parts for MTN Irancell***, which launched in 2006 and is now Iran's second-largest mobile-phone operator. ***"All the procedures and processes around procurement were established by MTN,"*** he said. He said the company ***agreed to allow its Iranian partners and MTN Irancell*** to set up a local Iranian company with the ***"basic" purpose of evading sanctions on Iran.*** ...

Reuters provided MTN with the names of four current MTN Group executives believed to have knowledge of the procurement of U.S. parts by MTN Irancell. MTN declined to make any of them available for interviews. ...

Kilowan's claims regarding how MTN Irancell obtained U.S. parts for its network ... were supported in documents and numerous interviews ... For example, *Reuters* reviewed an 89-page MTN Irancell document from 2008 that shows the telecom carrier was specifically interested in acquiring embargoed products. ... In a section on managing product-support agreements for third-party equipment, ***the MTN Irancell document states, "This should include embargo items."*** The document also includes ***lists of network equipment, including Cisco routers, Sun servers and products from HP.*** ... (*Id.* (emphasis added; formatting adjusted)).

620. *Reuters* "documented ... how Iranian telecoms - including the MTN joint venture – [] managed to obtain embargoed U.S. computer equipment through a network of Chinese, Middle Eastern and Iranian firms."¹⁹⁸ As *Reuters* put it, "[t]he Turkcell-MTN case offers further evidence that there are always companies willing to do business with a country even when it becomes an international pariah." *Id.*

621. MTN's technical assistance to Hezbollah, the Qods Force, and Regular IRGC had a devastating impact on the U.S. government's ability to protect Americans in Afghanistan from al-Qaeda and Taliban terrorist attacks. By helping to revolutionize the IRGC's communications capabilities, MTN helped Hezbollah, the Qods Force, and Regular IRGCs better conceal their communications with their proxies inside Afghanistan to make it nearly impossible for American counter-terror forces in Afghanistan to monitor the IRGC-backed terrorists attacking Americans

¹⁹⁸ Steve Stecklow and David Dolan, *Special Report: How An African Telecom Allegedly Bribe Its Way Into Iran*, *Reuters* (June 15, 2012).

in there. By making it easier for Hezbollah, the Qods Force, and Regular to securely communicate with one another, and the IRGC's proxies in Afghanistan, MTN made it easier for al-Qaeda and the Taliban to attack Americans – and they did. MTN accomplished this “communications concealment” assistance to Hezbollah, the Qods Force, and Regular IRGC which flowed through to al-Qaeda and the Taliban in at least three ways.

622. *First*, MTN acquired advanced American-made encryption technologies for Hezbollah, the Qods Force, and Regular IRGC, which flowed through to al-Qaeda and the Taliban. The terrorists used the MTN-acquired, U.S.-manufactured and embargoed technologies to encrypt their communications.

623. *Second*, MTN sourced more than one thousand (1,000) advanced, encrypted American smart phones each year from 2006 through 2017 that were intended to be used, and were in fact used, by Hezbollah, the Qods Force, and Regular IRGC, for terrorism targeting Americans. The American smart phones sourced by MTN for Hezbollah, the Qods Force, and Regular IRGC, were used to increase the effectiveness of IRGC-funded (including and Qods Force-funded) IEDs in Afghanistan by making it easier for terrorists to detonate them and harder for American counter-IED technologies to prevent their detonation by “jamming” them.

624. *Third*, MTN lied to the U.S. government about its ongoing cooperation with and work on behalf of Hezbollah, the Qods Force, and Regular IRGC. This furthered al-Qaeda's and the Taliban's terrorist campaign in Afghanistan by preventing the U.S. government from knowing and understanding what technology the terrorists had, and when it was obtained.

625. As alleged, MTN knew, or recklessly disregarded, that it was dealing with Qods Force fronts, but given the IRGC's designation as an FTO in 2019, MTN's ongoing relationship with two widely recognized IRGC fronts proves MTN deliberately chose to join the IRGC's,

including Hezbollah's and the Qods Force's, terrorist enterprise against the United States, which MTN self-evidently views as an acceptable cost of doing business.

626. MTN's ongoing refusal in August 2022 to immediately and unconditionally (as in weeks, not months or years) exit its joint venture with fronts for Hezbollah, the Qods Force, and Regular IRGC even after the IRGC had been designated as an FTO in April 2019, and nearly every other multinational corporation (aside from ZTE and Huawei) had withdrawn from such joint ventures with Iranian fronts nearly a decade earlier, further confirms that MTN meant to support Iran-backed terror all along. UANI's public pressure campaign demonstrates this. On February 29, 2012, for example, Ambassador Wallace released a public letter as follows:

[MTN] fails to respond to evidence of Iran's routine use of telecommunications equipment to illegally track, monitor, and in some cases arrest, detain, and torture Iranian citizens opposed to the current extremist regime. More specifically, [MTN] also fails to refute the fact that the Iranian regime, the majority 51% holder of Irancell and partner of MTN, "has exploited the network and communications of peaceful dissidents in Iran." Finally, [MTN] fails to respond to UANI's inquiries regarding multiple reports of collaboration by MTN Irancell and the Iranian regime ... MTN is a 49% shareholder of MTN Irancell, and the majority 51% is in turn owned by the Iranian regime. ***This means that MTN's "partner" in MTN Irancell is the Iranian regime. ...***

In addition, given MTN's relationship with the regime, MTN's assertion that it is a "liberating force," "enriching the lives" of Iranians is completely untenable. MTN cannot reasonably assert that the substantial profits it earns from its growing role in the Iranian telecommunications market are merely a byproduct of a larger altruistic goal to empower the citizens of Iran and the developing world....

Recent reports in the news media regarding MTN's Iran business further belie MTN's assertion that its business in Iran is altruistic or ethical in nature. For example ***MTN Irancell's other Iranian partial owner is the Mostazafan Foundation of Islamic Revolution, a "Bonyad" organization directly supervised by Iran's Supreme Leader. Both IEI and Mostazafan are closely linked to the regime's radical [IRGC]. ...*** [Emphases added.]

627. On March 28, 2012, Turkcell filed suit against MTN Group in United States District Court for the District of Columbia. *See* Compl. [Dkt. 1], *Turkcell İletişim Hizmetleri*

A.S. and East Asian Consortium B.V v. MTN Group, Ltd. and MTN International (Mauritius) Ltd., No. 1:12-cv-00479-RBW, (D.D.C. Compl. Filed Mar. 28, 2012) (“*Turkcell v. MTN*”).¹⁹⁹ Turkcell’s complaint alleged that MTN “violat[ed] ... the law of nations through bribery of sitting Iranian ... officials and trading influence to steal the first private Iranian Global System for Mobile Communications (“GSM”) license (the ‘License’) from Turkcell,” which included MTN’s “promis[e] [to] Iran [MTN would source] defense equipment otherwise prohibited by national and international laws” and MTN’s “outright bribery of high-level [] officials in both Iran and South Africa,” which “acts ... deliberately resulted in Turkcell losing its rightfully-won valuable telecommunications opportunity and in MTN’s taking over the License.”²⁰⁰

628. Turkcell also alleged that MTN Group engaged an IRGC-controlled company.²⁰¹

¹⁹⁹ Turkcell subsequently voluntarily dismissed the case to pursue the matter in South Africa. See Notice of Voluntary Dismissal (Dkt. 47) and Minute Order (Dkt. 48) in *Turkcell v. MTN*, No. 1:12-cv-00479-RBW (D.D.C. May 1, 2013).

²⁰⁰ Turkcell also alleged that, “[b]etween the end of 2004 and receiving the License in November 2005, MTN through ‘Project Snooker’ made at least five illegal bribes and trades in influence to government officials with the intention and belief that the bribes would cause the Iranian government to grant the License to MTN rather than Turkcell.” *Turkcell v. MTN* Complaint ¶ 9.

²⁰¹ See, e.g., *id.* ¶ 65 (“[To] establish[] itself within Iran[,] ... [MTN] reached out to ... Mr. Mohammed Mokhber, the Deputy President of a major “charitable foundation” controlled by the Supreme Leader of Iran, known as the Bonyad Mostazafan (“the Bonyad”), which is ... controlled by the Iran Revolutionary Guard Corps, the Iranian military complex formed by Iran’s Supreme Leader Ayatollah Ali Khamenei, which is believed to control approximately one third of the Iranian economy. ... The Bonyad reports directly to the Supreme Leader and MTN was confident that its relationship with Mr. Mokhber and the Bonyad he controlled provided direct access to the Supreme Leader. The Bonyad is well known for engaging in ‘Iran’s shadow foreign policy.’”). Similarly, Turkcell also alleged (at ¶ 86), that “[t]hroughout 2004 and 2005, MTN regularly met with ... the Bonyad [Mostazafan] and Sairan [i.e., IEI],” during which time MTN’s “goal was to entice those entities to support MTN and abandon Turkcell, on the promise that MTN had more to offer than Turkcell.” *Id.* ¶ 86. Turkcell continued: “The Bonyad and [IEI] responded exactly as MTN planned: They not only used political leverage to increase delay and shift Turkcell’s regulatory requirements, but also they directly began disengaging from their relationship with Turkcell. After mid-2005, the Bonyad and [IEI]’s involvement with Turkcell was merely a charade along the path to forming its venture with MTN.” *Id.*

629. Indeed, MTN remained defiant even though nearly every other major multinational corporation (aside from ZTE and Huawei) exited their own joint ventures with fronts for Hezbollah, the Qods Force, and Regular IRGC after the Bush and Obama administration ramped up sanctions enforcement in the 2000s. As Ambassador Wallace explained in May 2012, “despite the action of other responsible telecommunication companies, South African telecom company MTN continues to openly partner with sanctioned Iran entities affiliated with the brutal Iranian regime. *Companies like MTN deserve the condemnation of the American public and concerned citizens worldwide as well as the attention of this Congress, which should investigate MTN’s collaboration with the Iranian regime.* Nevertheless, UANI will continue to educate citizens and apply pressure against recalcitrant companies that pursue short-term profits at the expense of global security.”²⁰²

4. MTN Knowingly Assumed A Financial, Logistical, And Operational Role In The Taliban’s, Including The Haqqani Network’s, Terrorist Enterprise In Afghanistan, Directly And Indirectly Financing And Arming IRGC Proxy Attacks In Afghanistan And Iraq

i. MTN Made Protection Payments To The Taliban

630. MTN has become one of the world’s most valuable telephone companies by “wading into nations dealing with war, sanctions and strife.”²⁰³ Success in unstable markets, including Afghanistan, has yielded profits. MTN is now, due to this business model, “bigger by some measures than its U.S. counterparts.”²⁰⁴

631. MTN followed that model in Afghanistan. In mid-2006, MTN Group bought Areeba, a Lebanese telephone company that had recently won a license to provide cellular-

²⁰² Wallace May 17, 2012 Testimony (emphasis added).

²⁰³ Alexandra Wexler, *Telecom Giant Pushes Into Dangerous Areas*, Wall St. J. (Aug. 10, 2019).

²⁰⁴ *Id.*

telephone service in Afghanistan. MTN entered the Afghan market shortly thereafter and began as the country's third-largest provider (consistent with its status as the third entrant), well behind the two incumbents. But MTN grew quickly, and by late 2010 it had obtained an estimated 32% market share – the largest of Afghanistan's then-five cellular-phone providers. As MTN grew, it rebranded Areeba as MTN Afghanistan, and it expanded its geographical footprint throughout the country. By 2012, MTN had a presence in virtually every province in Afghanistan, including many that were under Taliban control or influence.

632. While MTN was achieving rapid growth in Afghanistan, the cellular-telephone sector provided a critical source of financing for the Taliban. As reported by the *Wall Street Journal* in 2010, telephone industry executives themselves “say operators or their contractors routinely disburse protection money to Taliban commanders in dangerous districts. That’s usually in addition to cash that’s openly passed to local tribal elders to protect a cell-tower site – cash that often also ends up in Taliban pockets.”²⁰⁵ “Coalition officers,” the article continued, “confirm that carriers make payments to the Taliban.”²⁰⁶ Those payments mirrored the protection money delivered by other Defendants. As terrorist-financing expert Thomas Ruttig documented, just as the Taliban raised “taxes” from international contractors doing business in Afghanistan, so too did it levy similar “taxes” on “the big telecom companies” like MTN.²⁰⁷

633. The logic behind MTN's protection payments partially matched the logic motivating the other Defendants. The MTN Defendants intended to harm American interests in

²⁰⁵ Yaroslav Trofimov, *Cell Carriers Bow To Taliban Threat*, Wall St. J. (Mar. 22, 2010). Mr. Trofimov has long served as one of the *Wall Street Journal*'s top terrorism-related reporters, and has extensive experience reporting from inside areas in which terroristic violence is widespread.

²⁰⁶ *Id.*

²⁰⁷ Thomas Ruttig, *The Other Side* at 20, Afghanistan Analysts Network (July 2009) (“*Ruttig, The Other Side*”).

Afghanistan, and supporting the Taliban allowed them to do so. In addition, MTN had economic motivations similar to those of the other Defendants. Specifically, the Taliban asked MTN to “pay monthly protection fees in each province, or face having their transmission towers attacked.”²⁰⁸ The going rate was “usually in the range of \$2,000 per tower, per month, but it depends on who controls the zone around each tower.”²⁰⁹ In some areas, MTN made payments to local Taliban commanders in exchange for protection. In others – such as Helmand and Kandahar – MTN operated in a Taliban-controlled environment in which protection “payments must go directly to Quetta.”²¹⁰ For example, one company confirmed to *Deutsche Presse Agentur* that it made \$2,000-per-tower monthly payments to the Taliban. The company’s owner posited: “You have to do it. Everybody does.”²¹¹

634. The Taliban conveyed its protection-money demands to MTN and other large cellular-phone providers via Night Letters. For example, the *Financial Times* reported in 2008 that Taliban commanders in Wardak Province had “sent letters to mobile phone companies demanding ‘financial support’ in return for operating” in Taliban-run areas.²¹² Those tactics were successful. One industry source estimated in 2009 that “every single one of the shadow provincial governors set up by the Taliban leadership council receives \$50,000 to \$60,000 in

²⁰⁸ *Crime & Insurgency* at 32.

²⁰⁹ *Id.*

²¹⁰ *Id.*; see *id.* (one company admitting it “routinely sen[t] a representative to Pakistan to pay off the Taliban leadership”).

²¹¹ Can Merey, *How The Taliban Has Turned Extortion Into A Gold Mine*, *Deutsche Presse-Agentur GmbH* (June 4, 2009).

²¹² Jon Boone, *Telecom Chief Says Rivals Pay Taliban Protection*, *Fin. Times* (June 9, 2008).

protection money each month alone from the telecommunications sector, the largest legal growth market in Afghanistan.”²¹³

635. The Taliban itself confirmed that practice. After the *Financial Times* obtained a copy of a Taliban Night Letter demanding protection payments from cellular-phone companies in Wardak Province, the reporter called the telephone number listed as the point of contact in the Taliban’s letter. A “local Taliban official” answered and confirmed that “two companies had responded to their demands” by agreeing to pay. On information and belief, MTN was one of them. The Taliban explained: “When a company sets up they have to pay tax to the government of Afghanistan. . . . We are the government here and they must pay tax to us.”²¹⁴

636. MTN was a particularly aggressive practitioner of protection payments. Rather than invest in expensive security for its transmission masts, MTN purchased cheaper “security” by buying it from the Taliban. Indeed, MTN declined to use armed guards to protect its towers. Without paying for physical security, MTN both had the free cash flow and the incentive to buy peace with the Taliban. The CEO of one of MTN’s largest competitors, Roshan, alleged as much in 2008. According to an interview the CEO gave to the *Financial Times*, other “phone companies in Afghanistan [were] bowing to criminal and Taliban demands to pay protection money to avoid the destruction of their transmission masts.” *Id.* In the interview, Roshan’s CEO continued: “I believe the competition is paying money, but we don’t do that.” *Id.* Of Roshan’s four largest competitors, three of them denied the accusation on the record. Only “MTN, the South African based multinational phone company, was not available for comment.” *Id.*

²¹³ Can Merey, *How The Taliban Has Turned Extortion Into A Gold Mine*, Deutsche Presse-Agentur GmbH (June 4, 2009).

²¹⁴ Jon Boone, *Telecom Chief Says Rivals Pay Taliban Protection*, *Fin. Times* (June 9, 2008) (“*Rivals Pay Taliban Protection*”).

637. MTN’s statements reflect its practice of paying off terrorists. Because MTN paid the Taliban, it was, in MTN’s own words, “‘not a target.’”²¹⁵ According to MTN Afghanistan, “it’s enough for a driver to show at a Taliban checkpoint a company letter stating that equipment aboard the truck belongs to MTN and not to the U.S. forces.” *Id.*

638. MTN negotiated its protection payments in direct discussions between MTN Afghanistan’s security department and Taliban commanders. MTN’s security department consisted of roughly 600 total staff in Afghanistan, which included both local Afghan employees of MTN Afghanistan and a South African security component from MTN Group. The security department consisted of three different layers: provincial, regional, and a Tactical Operations Center in Kabul. Security personnel throughout those levels orchestrated payoffs to the Taliban. For example, one high-ranking MTN Afghanistan official conducted at least 38 telephone negotiations (which he recorded) with Taliban officials from 2007-2014, in which he engaged in so-called “security coordination” with the insurgency. The MTN employees who witnessed those conversations knew they were illegal, so they typically went to the roof of MTN Afghanistan’s Kabul headquarters building – where they could maintain absolute privacy – to conduct their Taliban negotiations in secret. In addition, on at least one occasion, MTN negotiated its payments at an in-person meeting held with Taliban officials near Quetta, Pakistan. MTN employees in Afghanistan understood that those negotiations involved MTN agreeing to make both cash payments and in-kind bribes (including equipment) to the Taliban.

639. MTN’s practice of making protection payments to the Taliban extended to the Haqqani Network. From at least 2010 through 2016, MTN operated towers in Haqqani-controlled territory in southeast and eastern Afghanistan, and it purchased security for those

²¹⁵ Yaroslav Trofimov, *Cell Carriers Bow To Taliban Threat*, Wall St. J. (Mar. 22, 2010).

towers by paying the Haqqani Network. The Network's chief financial operative, Nasiruddin Haqqani, oversaw those payments, and they typically occurred on a semi-annual basis.

640. The U.S. government strongly opposed MTN's practice of paying the Taliban. ISAF's leadership was aware of cell phone companies making protection payments to the Taliban and pressured the companies to stop. On information and belief, the U.S. government exerted that pressure in direct discussions between the U.S. government and MTN, and also through the Afghan Ministry of Communications. On one occasion, an ISAF commander raised the issue directly with President Karzai. In such conversations, ISAF's leadership specifically rejected the argument that protection payments represented an acceptable price of MTN maintaining its network in Afghanistan. ISAF and the Afghan government warned MTN Afghanistan that its business practices were supporting the insurgency and were threatening Coalition forces, and both entities instructed MTN to stop. MTN refused.

641. MTN supplied the Taliban with more substantial assistance than its competitors did. MTN's 2006 entry into Afghanistan set the stage for the Taliban's cellular-tower rackets by adding another participant to the Afghan cellular marketplace. Until that point, the Taliban's ability to extract money from the two incumbent providers had been limited. Once MTN emerged in 2006, it became the third cellular company in Afghanistan, which gave the Taliban additional leverage to execute on its protection racket. That is because, with MTN agreeing to pay the Taliban, the Taliban were free to follow through on its threats against other companies without the risk that doing so would cut off all cellular service in Afghanistan – service on which the Taliban itself relied. Indeed, because Taliban fighters commonly preferred to use MTN's network for their own communications, the Taliban did not want to destroy MTN's network.

642. A review of available cell-tower attack data supports the same conclusion. Plaintiffs have analyzed all the available purported U.S. military Significant Activities reports, as published online, that describe attacks between 2004 and 2010 against or in the immediate vicinity of a cellular tower in Afghanistan. The data shows a clear disparity between MTN and its two main competitors, Roshan and Afghan Wireless Communication Company (“AWCC”). From 2004 to 2009, AWCC and Roshan suffered at least 6 and 7 attacks on their towers, respectively, whereas MTN – which did not even pay guards to protect its towers – faced only 1 (non-lethal) attack. The disparity is consistent with Roshan’s accusation that MTN paid protection money to the Taliban.

643. That attack disparity existed despite MTN’s and Roshan’s deployment of transmission masts at similar times in similar locations. For example, Roshan’s CEO cited to the *Financial Times* an instance on May 14, 2008, in which the Taliban attacked one of Roshan’s towers in Wardak Province, yet two similar nearby towers (including one belonging to MTN) were not attacked.²¹⁶ The most likely explanation for the difference is that MTN had paid protection money, whereas Roshan had not. Indeed, in 2009, Roshan maintained company rules that prohibited it from paying protection money to terrorists. Because Roshan refused to pay, the Taliban destroyed 18 of Roshan’s towers in and around the 2009 Afghan elections.

644. The senior MTN Afghanistan security official who oversaw many of MTN Afghanistan’s protection payments to the Taliban reported directly to the head of MTN Group’s head of business risk management, in Johannesburg, South Africa. MTN Group was specifically aware of, and approved, MTN Afghanistan’s practice of paying the Taliban for security. In fact, MTN Group compensated MTN Afghanistan’s security team with cash bonuses reflecting its

²¹⁶ *Rivals Pay Taliban Protection.*

success at resolving “security issues” involving the Taliban. Those bonuses typically had three levels: Level 1 (\$1,500, for local operatives); Level 2 (\$5,000, for regional operatives); and Level 3 (\$10,000, for national operatives). The head of MTN Afghanistan’s security group received roughly \$66,000 in such bonuses during the relevant timeframe, which specifically compensated him for negotiating with the Taliban successfully. MTN Group even gave him an award for best “display[ing] the Group’s values in MTN Afghanistan.”

645. MTN’s overall payments to the Taliban reached tens, if not hundreds, of millions of dollars. Applying the standard rate of \$2,000 per tower per month to MTN’s collection of roughly 1,300 towers yields an estimated payment of \$2.6 million per month. At that rate, MTN’s payments from 2007 through 2016 well surpassed \$100 million.

ii. MTN Supported The Taliban By Deactivating Its Cellular Towers At Night

646. MTN also provided material support to the Taliban by deactivating its cell towers at the Taliban’s request. In or about 2008, the Taliban began demanding that Afghanistan’s major cellular-phone providers switch off their towers at night. The Taliban justified that demand by arguing that Coalition forces were “using the cellular networks to track its insurgents throughout the war-torn country.”²¹⁷ Coalition forces, a Taliban spokesman stated, were “misusing the cell towers for their intelligence works.”²¹⁸ Because the Taliban believed that shutting down nighttime service would impede Coalition intelligence efforts, it demanded that

²¹⁷ Paul Vecchiatto, *MTN Concerned By Afghanistan Threats*, ITWeb Cape Town (Feb. 28, 2008) (“*MTN Concerned By Afghanistan Threats*”), <https://www.itweb.co.za/content/dgp45MaYRYZMX918>.

²¹⁸ Indira A.R. Lakshmanan, *Fighting The Taliban With Cellphones*, N.Y. Times (Mar. 23, 2010).

the cellular-phone companies deactivate their transmission masts from 5 p.m. until 3 a.m. Later, the Taliban insisted that the companies keep their masts deactivated until 6:30 a.m.

647. MTN granted the Taliban's requests. In early 2008, MTN Group issued a statement that it was "aware of reports of the Taliban communicating a need for mobile operations to be suspended at certain times during the night in sensitive areas. We are evaluating the situation and liaising with our executives and the relevant authorities in Afghanistan."²¹⁹ The "executives" apparently decided to accommodate the Taliban's "need" and shut down MTN's transmission masts at night. MTN and others, the *Wall Street Journal* reported in 2010, "strictly abide[d] by Taliban hours in several provinces, going off air precisely at 5 p.m. and going back on at 6:30 a.m."²²⁰ And when the Taliban ordered cellular-phone companies in Helmand to "switch off the signal," MTN Afghanistan's head of legal and government affairs told the media: "We decided to obey the orders and we have been shut down since yesterday."²²¹ Since 2008, MTN's policy has remained consistent: it has followed the Taliban's directives and switched off its transmission masts for the Taliban's benefit – typically at night.

648. MTN shut down its towers for the same reason it paid protection money: to maintain good relations with the Taliban. MTN made no effort to hide its motivation in that regard. When asked about shutting down its network, MTN Afghanistan's head of legal and government affairs explained that the company could not "afford to be seen as siding with the Afghan government against the Taliban . . . 'You should not give a justification to the others

²¹⁹ *MTN Concerned By Afghanistan Threats*.

²²⁰ *Cell Carriers Bow To Taliban Threat*.

²²¹ Agence France Presse, *Taliban Shut Down Cell Phones In Afghan Province* (Mar. 24, 2011).

that you are favoring the government – and you have to prove in words and in deeds that you are neutral.”²²²

649. MTN went to great lengths to maintain its “neutrality” and do what the Taliban asked of it. Even in 2011, after President Karzai issued a decree formally demanding that MTN (and its competitors) reactivate their towers at night, MTN refused the recognized government’s directive and continued to follow the Taliban’s requests. One executive summed up MTN’s (and others’) refusal to follow President Karzai’s directive: “We’re not going to turn on our masts and become part of the army of the Afghan government.”²²³ By shutting down its towers, MTN decided, it could reduce the risk that the Taliban would threaten MTN’s commercial interests.

650. The ATFC gathered evidence confirming that MTN was switching off its transmission masts at night to comply with Taliban demands. Based on intelligence reporting, wire intercepts, and interviews with MTN sources, the ATFC concluded that MTN Afghanistan was deactivating its cell towers in coordination with the Taliban. The justification offered by MTN Afghanistan employees was, again, financial: turning off the towers helped MTN save money by avoiding the need for MTN to invest in expensive security or to rebuild its towers. The ATFC observed that the security threat MTN faced was not primarily to its employees; it was to equipment that MTN did not want to spend the money to protect or rebuild.

651. MTN Afghanistan implemented tower shutdowns through a secretive process that originated with its security team. The head of MTN Afghanistan’s security division would negotiate with the Taliban to determine which towers (called “Base Transceiver Stations” by MTN’s technical team) to shut down, and at which times. Then, based on information received

²²² *Cell Carriers Bow To Taliban Threat*.

²²³ Jon Boone, *Taliban Target Mobile Phone Masts To Prevent Tipoffs From Afghan Civilians*, *The Guardian* (Nov. 11, 2011).

from the Taliban, MTN's security team relayed instructions to MTN Afghanistan's technical team directing them to implement the shutdowns. The instructions pinpointed the particular quadrant(s) within particular MTN towers' coverage areas in which Taliban operatives were located, specifying that MTN should turn off the signal within those quadrants. That enabled MTN to satisfy the Taliban's demands while also allowing MTN to continue earning revenue from customers in the other quadrants – and also to deceive the government about the extent of its shutdown. MTN employees further avoided memorializing these instructions over company email or in memos; they instead used phone calls or text messages with the purpose of avoiding a paper trail that would document their cooperation with the Taliban.

652. At all relevant times, MTN Group was aware of, and approved, MTN Afghanistan's practice of shutting down its towers to comply with the Taliban's requests. MTN Afghanistan would not have maintained that policy without specific buy-in from MTN Group's senior management in South Africa.

653. MTN's conduct strengthened the Taliban and undermined U.S. counterinsurgency efforts. By 2010, the Taliban was "using the cellphone system as an instrument of war against the Afghan government and the U.S.-led coalition."²²⁴ The insurgents, one Army officer told the *New York Times*, used MTN's cell towers "as a weapons system" against Coalition forces.²²⁵ Indeed, cell phones were crucial to the Taliban – they provided a convenient form of communication and helped insurgents coordinate attacks – but they also came with two major downsides. First, U.S. intelligence tracked the Taliban's phone signals and used them to locate

²²⁴ *Cell Carriers Bow To Taliban Threat*.

²²⁵ Indira A.R. Lakshmanan, *Fighting The Taliban With Cellphones*, N.Y. Times (Mar. 23, 2010).

high-level targets for capture-or-kill missions. Second, cell phones provided Afghan civilians with the ability to call Coalition tip lines and provide valuable human intelligence.

654. Nighttime deactivation was the Taliban's solution to both problems. U.S. Special Forces typically execute high-value raids at night, and deactivated cell signals impeded those missions by making the insurgent targets harder to track. That was the Taliban's stated rationale for demanding nighttime signal deactivation: its spokesman argued that Taliban fighters had "been increasingly targeted by foreigners recently and we know they are using the services of these phone companies against us."²²⁶ As another Taliban spokesman explained publicly, the Taliban viewed the "cutoffs as a line of defense," in which its "'main goal is to degrade the enemy's capability in tracking down our mujahedeen."²²⁷ Consistent with that statement, *AFP* reported that "Taliban militants regularly demand that mobile phone companies switch off their networks at night, fearing that NATO-led forces can track them through phone signals."²²⁸

655. Similarly, nighttime deactivation obstructed Coalition efforts to gather human intelligence. Cell phones provided a key conduit for Afghan civilians to pass intelligence to Coalition personnel. But as the U.S. military director of the Telecommunication Advisory Team explained, "[i]f the masts are off Afghans can't report anything . . . If you see an insurgent you can't call the police to say check this out."²²⁹ And Afghan informants were "usually reluctant to call in tips during daytime, when they can be spotted by Taliban sympathizers."²³⁰ Human

²²⁶ Agence France Presse, *Taliban Shut Down Cell Phones In Afghan Province* (Mar. 24, 2011) ("*Taliban Shut Down Cell Phones*").

²²⁷ Alissa J. Rubin, *Taliban Using Modern Means To Add To Sway*, N.Y. Times (Oct. 4, 2011).

²²⁸ *Taliban Shut Down Cell Phones*.

²²⁹ Jon Boone, *Taliban Target Mobile Phone Masts To Prevent Tipoffs From Afghan Civilians*, The Guardian (Nov. 11, 2011).

²³⁰ *Cell Carriers Bow To Taliban Threat*.

intelligence thus typically flowed to the Coalition at night. By agreeing to shut down its transmission masts, MTN knowingly deprived Coalition forces of that vital intelligence.

656. In 2010, *CBS News* reported on this so-called “détente” between the Taliban and large mobile-phone companies, including MTN. “The phone companies shut down their cell towers at night, preventing local residents from discreetly calling coalition military tip lines. In exchange, Taliban militants don’t target the costly cell towers with explosives.”²³¹ The trade was a major strategic victory for the Taliban. As Roshan’s COO explained in trying to justify a similar decision: “We play by their rules; we don’t like to play around when people’s lives are at stake. . . . From a political perspective, it’s quite a coup for them.”²³²

657. MTN’s tower shutdowns substantially contributed to the Taliban’s ability to commit the attacks that killed and injured Plaintiffs. The Taliban targeted its shutdown orders at key districts and provinces with tactical importance for ongoing Taliban operations. As MTN knew, tower deactivation in those areas impeded Coalition forces from locating Taliban operatives and degraded the Coalition’s ability to interdict Taliban ongoing attacks. Indeed, the U.S. intelligence benefits gleaned from active cell towers were so potent that ISAF often executed operations designed specifically to induce Taliban operatives to use their phones. By the same token, the operational impact of MTN’s tower-shutdown policy was so extreme that ISAF, U.S. Embassy, and Afghan government personnel repeatedly pressured MTN to stop. ISAF command considered such shutdowns to be a significant threat to U.S. counterinsurgency efforts. And those shutdowns occurred in the key provinces and districts in which Plaintiffs (or their family members) were operating when they were killed and injured. By defying the U.S.

²³¹ Alex Sundby, *Afghan Cell Carriers Follow Taliban Rules*, CBS News (Mar. 24, 2010).

²³² *Id.*

government and obeying the Taliban in the contested areas in which the insurgents were fighting Americans, MTN materially supported the Taliban attacks that killed and injured Plaintiffs.

658. The U.S. government tried to address those problems by encouraging Afghanistan's cellular-phone providers to move their transmission masts onto secure U.S. bases. As the U.S. government explained in proposing the idea, securely located transmission masts would be difficult for the Taliban to attack – and could thus eliminate the putative reason MTN was deactivating its cell towers when the Taliban told it to. Roshan, according to a purported 2009 U.S. State Department cable (as published online), was “keen to develop this partnership with the USG and sees it as a way to promote mutual security, communications, and commercial strategies for Afghanistan.”²³³ MTN, by contrast, refused to participate and declined even to join Roshan and AWCC at the U.S. government-brokered meeting to discuss the idea.

659. Neither the U.S. government nor the Afghan government ever condoned or conveyed approval of MTN's tower-shutdown policy. Although news reports on occasion quoted individual Afghan government officials suggesting a resignation to the reality of MTN's shutdown policy, the official Afghan government position – conveyed at in-person meetings held with MTN, including at least one with President Karzai himself – was that cell-phone companies must keep their towers active at night. The U.S. government was even more strongly committed to that position. ISAF leadership especially rejected the suggestion that MTN's conduct represented an acceptable way of protecting its network. ISAF expected MTN to keep its towers on, invest in security to protect them itself rather than paying the Taliban, and ultimately rebuild

²³³ U.S. State Dep't Cable ¶ 11, *Using Connection Technologies To Promote US Strategic Interests In Afghanistan* (July 23, 2009).

them if necessary. ISAF considered that course of action not only feasible, but mandatory for a company like MTN reaping profits in an insurgency-afflicted country like Afghanistan.

5. MTN's Assistance To Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, And The Taliban, Comports With MTN's Historical Business Practices In International Markets

660. MTN's conduct above reflected a willingness to support America's enemies as a way to increase profits in Iran.

661. **MTN Aided the IRGC's Terroristic Violence against Iranian Pro-Democracy Demonstrators.** MTN enabled the terroristic violence deployed by IRGC agents against peaceful pro-democracy and human rights protestors in Iran during the 2009 uprising popularly known as the "Green Revolution."

662. As the *L.A. Times* explained at the time, while Iran "brac[ed] for further confrontations between security forces and supporters of Mousavi ...[,] [o]ne of the country's main cellphone operators, Irancell, co-owned by South Africa's MTN, warned customers [] that it would be suffering unspecified 'technical' problems over the next three days, which coincide[d] with the anticipated unrest."²³⁴ MTN was lying to its customers and the world – there were no "technical" problems but, rather, simply the IRGC's desire to shut down any avenue for mass democratic mobilization against it – which MTN happily obliged.

663. MTN went beyond merely lying to its customers when it shut down its network at the request of the IRGC. MTN actively aided the IRGC by helping it develop sophisticated tools for monitoring, eavesdropping, and surveilling targets. MTN's technical services for the IRGC did not merely benefit its domestic regime suppression; the exact same functions also benefit

²³⁴ Borzou Daragahi, *Iran Court Warns Against Criticizing Proceedings*, L.A. Times (Aug. 3, 2009), 2009 WLNR 14945080.

foreign intelligence gathering, surveillance, and communications – critical competencies relevant to the success of a terrorist attack against Americans in Iraq.

664. **MTN Aided Terrorists in Nigeria.** MTN also aided violent actors in Nigeria. On or about October 26, 2015, the Nigerian Communication Commission fined MTN Group \$5.2 billion for failing to meet a deadline to disconnect 5.1 million unregistered subscribers in Nigeria. Nigeria imposed the deadline on all cellular operators in the country due to evidence that unregistered phones were facilitating the activities of criminal gangs and terrorists, including Boko Haram. The requirements that MTN violated, the *Wall Street Journal* reported, were “meant to combat terrorism.”²³⁵ MTN eventually negotiated the criminal fine down to \$1.67 billion and agreed to pay it in seven installments.

6. MTN’s Acts In Furtherance Of The Conspiracy Had A Substantial Nexus To The United States

665. MTN’s joint venture with the IRGC and its related assistance for al-Qaeda and the Taliban, relied on significant contacts with the United States. MTN Group was a key player in orchestrating both those U.S. contacts and MTN’s material support to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban.

666. Even while MTN Group was reaching into the United States to launch a multifaceted campaign to facilitate the flow of U.S. dollars to and from MTN Irancell, its CEO continued expressing his contempt for the United States. Instead of exiting MTN Group’s and MTN Dubai’s choice to join the Conspiracy with the IRGC, MTN Group’s President and CEO defiantly pronounced that “U.S. sanctions should not have unintended consequences for non-

²³⁵ Alexandra Wexler, *Nigeria Reduces MTN Group Fine By \$1.8 Billion*, Wall St. J. (Dec. 3, 2015).

U.S. companies.”²³⁶ This public statement by MTN Group’s President and CEO furthered the IRGC Conspiracy because it concealed the existence of the Conspiracy while simultaneously releasing specific IRGC disinformation.

667. MTN Group also connected ZTE’s and Huawei’s support of the IRGC Conspiracy to the United States by obtaining technology and vital operational support in reliance on U.S. contacts. MTN Group and MTN Dubai orchestrated a complex scheme to surreptitiously supply technology and operational support for MTN Irancell through various U.S. agents. In doing so, MTN Group and MTN Dubai tied MTN’s unlawful conduct to the United States in several ways.

i. MTN’s Conduct Targeted the United States

668. MTN’s provision of material support to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, was expressly aimed at the United States. At all relevant times, MTN knew that Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, were targeting the United States. Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, did not conduct an indiscriminate terrorist campaign that merely injured Americans by chance. Instead, Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, directed attacks at *Americans* with the specific intent of killing *Americans* in particular – so that they could inflict pain in the United States and influence U.S. policy. As the Treasury Department stated when it announced the Qods Force’s designation as a SDGT in 2007, “the Qods Force provides lethal support in the form of weapons, training, funding, and guidance to select groups of Iraqi Shi’a militants who target and kill Coalition ...

²³⁶ Stecklow, *How A Telecom Giant Got Round Sanctions On Iran*, *supra*.

forces...”²³⁷ Hezbollah’s, the Qods Force’s, Regular IRGC’s, al-Qaeda’s, and the Taliban’s, including its Haqqani Network’s, ultimate, shared, publicly stated goal was to effect a withdrawal of American forces from Afghanistan and the broader Middle East. Each terrorist attack that killed and injured Plaintiffs was part of that campaign of anti-American terrorism.

669. MTN also knew, based on conversations with U.S. officials, that it was assuming an active role in an IRGC, including Qods Force, plot to develop cash flow and to source vital dual-use components for Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban.. MTN further knew of the critical importance that communications and computing technology plays for terrorists.

670. When MTN sourced embargoed technology that the United States had publicly declared could benefit IRGC’s, including Qods Force, efforts to kill others, it intentionally helped arm terrorists it knew were targeting the United States. Indeed, the IRGC’s, including the Qods Force’s, direct statement in their contract with MTN obligated MTN to help the IRGC, including its Hezbollah Division and Qods Force, protect Iran’s “security.” MTN at all times knew or recklessly disregarded that “security” was a euphemism for IRGC, including Qods Force, terrorist operations outside of the territorial borders of Iran. When MTN obtained the technology requested by its partners in the IRGC, including its Hezbollah Division and Qods Force, MTN targeted the United States by helping the terrorists improve their bombs, rockets, communications, and intelligence gathering.

671. Although MTN’s primary motivation for assisting the IRGC, including its Hezbollah Division and Qods Force, was financial, it also intended to harm Americans in

²³⁷ U.S. Treasury Dep’t, *Fact Sheet: Designation of Iranian Entities and Individuals for Proliferation Activities and Support for Terrorism* (Oct. 25, 2007).

Afghanistan. One reason MTN cooperated with the IRGC, including its Hezbollah Division and Qods Force, was to align itself with their effort to drive Americans out of the country. MTN had two distinct but related reasons for desiring that outcome.

672. *First*, MTN intended to harm Americans because it decided that was the necessary price of maintaining a good relationship with the Ayatollah and the IRGC, including its Hezbollah Division and Qods Force. The Ayatollah and the IRGC, including its Hezbollah Division and Qods Force, were explicit – both in public, and in conversations with MTN – that it wanted MTN’s financial and technical help in fighting against U.S. forces in particular. Thus, for MTN to achieve its business objectives vis-à-vis its joint venture partners the Ayatollah and the IRGC, including its Hezbollah Division and Qods Force, MTN needed to disassociate itself from the United States and prove that it could deliver value to the IRGC’s terrorist campaign against U.S. forces in Afghanistan.

673. *Second*, MTN Group’s support for attacks against U.S. citizens by the Joint Cells advanced the foreign-policy interests of MTN Group’s most important business partner, the Bonyad Mostazafan and IEI, which MTN at all times knew to be IRGC, including Qods Force, fronts.

674. MTN Group depends on its partnership with the Ayatollah and the IRGC, including its Hezbollah Division and Qods Force. As of 2012, Iran was MTN’s fastest growing market and its third largest source of revenue overall. Today, Iran is MTN’s second-biggest market by subscribers. MTN Group’s financial incentive to satiate the Ayatollah and its IRGC, including Qods Force, partners has led it to take a number of illegal steps to assist the Iranian

regime. Three South African investigative journalists summarized these acts in an informative headline, “MTN [is] in bed with Iran’s military.”²³⁸

675. MTN Group cooperates with the Ayatollah, and the IRGC, and including the Qods Force, despite knowing that the Ayatollah, and the IRGC, and including the Qods Force, are collectively the world’s worst sponsor of anti-American terrorism.

676. MTN Group’s agreement to aid the IRGC, including its Hezbollah Division and Qods Force, served the IRGC’s, including the Qods Force’s, agenda of inflicting death and injury on U.S. forces. It also fulfilled MTN Group’s contractual obligation to engage in “defensive, security and political cooperation” with its IRGC, including Qods Force, partner.²³⁹ Such cooperation offered MTN Group additional motivation for becoming joint venture partners with the IRGC, including its Hezbollah Division and Qods Force. MTN’s support for the IRGC, including its Hezbollah Division and Qods Force, did not merely grow its profits by allowing it to obtain the Irancell business in the first instance; it also benefited MTN’s business by inflicting harm on an enemy (the United States) of MTN’s most lucrative business partner (the IRGC, including its Hezbollah Division and Qods Force, fronts that controlled MTN Irancell) in order for MTN to curry Iranian favor to gain market share for a potentially uniquely lucrative telecom and communications market in Iran.

ii. From 2012 Through 2019, MTN Group Regularly Reached Into The United States In Order To Unlock The U.S. Financial System So That MTN Group Could Repatriate Hundreds Of Millions Of Dollars Out Of MTN Irancell

677. MTN Group and MTN Dubai regularly engaged in large six- and seven-figure U.S. dollar transactions that flowed through the New York financial system before leaving the

²³⁸ Craig McKune et. al, *MTN In Bed With Iran’s Military*, Mail & Guardian (Feb. 10, 2012).

²³⁹ Exhibit A, MTN-Irancell Consortium Letter Agreement § 8 (Sept. 18, 2005).

United States to flow into accounts controlled by an IRGC “buffer” such as an agent, operative, cut-out, front, and Orbit companies.

678. MTN Group and MTN Dubai’s use of the New York financial system was not incidental. On information and belief, beginning on or about 2012 and continuing through on or about 2019, MTN Group, MTN Irancell, and MTN Dubai routinely relied upon banks in New York to manage the cash flow of MTN Group, MTN Dubai, and MTN Irancell, which was its most important (and cash-intensive) investment in the Middle East.

679. MTN Group established banking relationships with U.S. financial institutions and multinational financial institutions with U.S.-based subsidiaries or offices no later than 2013.

680. For example, MTN Group disclosed that it has a relationship with the Bank of New York, located at 101 Barclay Street, New York, NY 10286, as its depository bank. Similarly, in 2015, MTN Group disclosed its relationship with Citibank, whereby it guaranteed a syndicated loan facility worth \$1 billion, the same facility from which MTN International (Mauritius) Limited, the MTN Group subsidiary used to make corrupt payments to Iranian officials, had drawn \$670 million.

681. Following the easing of sanctions, in January 2016, MTN focused on repatriating funds from Iran. Indeed, MTN Group saw the easing of sanctions as an opportunity to “normalize” its repatriation of monies from MTN Irancell.

682. On October 24, 2016, MTN Group admitted that “MTN has commenced the repatriation of funds from MTN Irancell to MTN Group.”²⁴⁰ On December 14, 2016, “Bloomberg report[ed] that MTN Group ... extract[ed] several hundred million dollars with the

²⁴⁰ MTN Group Ltd., Mtn Group Limited - Quarterly Update For The Period Ended 30 September 2016, South African Company News Bites – Stock Report (Oct. 24, 2016).

help of European banks, and it [was] looking to take a total of around USD1 billion by the end of March 2017,” which “include[d] a *USD430 million loan repayment from MTN* Irancell.”²⁴¹

683. The MTN Irancell profits that MTN Group withdrew covered the period when nearly every Plaintiff was injured. When MTN Group coordinated a global strategy to facilitate the repatriation of its MTN Irancell profits, MTN Group reached into the United States to obtain an enormous benefit – the money it made – that was itself the motivation for the terrorist finance that killed and injured Plaintiffs.

684. On information and belief, MTN Group utilized its banking relationships with U.S. financial institutions and/or financial institutions with U.S. subsidiaries or offices, including but not limited to the Bank of New York and Citibank, to facilitate the repatriation of funds from MTN Irancell to MTN Group.

685. Each time MTN Group and MTN Dubai used New York’s financial system, they did so in a context where they benefited from the New York financial system, and New York laws, and they knew that the New York financial system imparted extra value to every transaction based upon its stability and reputation.

iii. MTN Group Facilitated A \$400,000 Bribe That Flowed Through The New York Financial System To A Cut-Out For The IRGC And Into The Budget Of Hezbollah, The Qods Force, And Regular IRGC

686. MTN Group’s U.S. contacts were essential to the initial bribe that allowed MTN Group to pilfer the Irancell license from Turkcell in the first instance and was the proximate and but-for cause of MTN Group’s and MTN Dubai’s subsequent ability thereafter to assist the

²⁴¹ CommsUpdate, MTN Extracts First Cash From Iran (Dec. 14, 2016), 2016 WLNR 38124973.

IRGC, including its Hezbollah Division and Qods Force's, terrorist enterprise, and join the Conspiracy.

687. MTN Group relied upon bank accounts in New York to complete the \$400,000 wire that MTN Group sent to a recipient in 2007 who acted on behalf of the IRGC, including its Hezbollah Division and Qods Force. That payment depended upon MTN Group's use of bank accounts in New York, which cleared the dollar transaction.

688. MTN Group caused the issuance of the \$400,000 wire to the cutout for the IRGC, including its Hezbollah Division and Qods Force, also aided the IRGC's, including the Qods Force's, efforts to covertly obtain U.S. dollars – the vital common currency of terrorist finance – to fund al-Qaeda and Taliban attacks against Americans in Afghanistan and Joint Cell attacks against Americans in Iraq.

iv. MTN Group And MTN Dubai Conspired To Provide, And Did Provide, A Stable, Robust, And Devastating Pipeline Of Illicitly Acquired State-of-the-Art American Technologies To Hezbollah, The Qods Force, And Regular IRGC, Including Untraceable American Smartphones

689. MTN Group's co-conspirators have already confessed to the crimes they committed in coordination with MTN Group. For example, Mohammad Hajian testified "that he sold super-computers worth about \$14-million to 'a South African cellphone company in Iran [a reference to MTN]', rather than to the regime itself." Rowan Philp and Craig McKune, *US Trial Turns Heat On MTN*, Mail & Guardian (Feb. 15, 2013). At the time, his "alleged co-conspirator [was] also on trial in the US on charges that he serviced embargoed US technology for a 'front company' of MTN Irancell." *Id.*

690. Like MTN Group and MTN Dubai, Mr. Hajian's legal "memorandum" "stated that the network was geared solely for a deal with MTN Irancell: 'All the merchandise was for non-military use and was intended to facilitate a joint venture between a South African cellphone

company and a non-governmental Iranian entity related to the provision of civilian cellular telephone service within Iran.”

691. United States District Judge Virginia Hernandez-Covington rejected the suggestion that MTN Irancell was a civilian phone company that was not under the control of the IRGC, and “ruled that the “[e]nterprise level server”] equipment sold to MTN Irancell in 2009 ‘could be dangerous’ in Iran, whether controlled by the government or by MTN Irancell.” *Id.*

692. Federal “[p]rosecutors” also rejected the suggestion that MTN Irancell was a civilian phone company that was not under the control of the IRGC, and told the district court “that the [‘e]nterprise level server’] equipment sold to MTN Irancell in 2009 could have military applications and be used to spy on citizens.” *Id.* Prosecutors explained: “Even if used by [MTN] Irancell now, Iran could redeploy the equipment at any time ... The equipment is capable of being used by Irancell, or others, to access private information about subscribers and possibly communications content.” *Id.* Indeed, “[t]he equipment Hajian was found to have illegally sold included a Sun Microsystems M9000 ‘enterprise level server, the largest and most powerful Unix processor that Oracle Sun sells,” and a “Hitachi Data Systems array,” which prosecutors “described as having the capacity to support various applications and ‘store vast amounts of data useful for large companies and [defense] departments.’” *Id.*

693. After pointedly noting Judge Hernandez-Covington’s ruling that the provision of U.S.-sold enterprise level server equipment to MTN Irancell “could be dangerous,” the *Mail & Guardian* journalists who followed Mr. Hajian’s trial also rejected the suggestion that MTN Irancell was a civilian company rather than an IRGC front:

In any event, Hajian’s assertion that Irancell was a civilian, non-governmental partnership was *inaccurate*. Although MTN owns 49% of the company, the balance is held by a consortium owned by two state-linked partners. The first, the purportedly charitable Bonyad Mostazafan Foundation, is *understood to be*

controlled by the Iran Revolutionary Guard and the second, the state-owned defence company Sairan, reports directly to Iran's minister of defence. (*Id.*)

v. MTN Obtained U.S. Technology For The Benefit Of Hezbollah, The Qods Force, And Regular IRGC

694. MTN's U.S. contacts were essential to the technological assistance it provided to the Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban. At all relevant times, MTN relied upon U.S. agents to illegally source dual-use technology from the United States that benefited the IRGC's terrorist enterprise, including attacks against Americans in Afghanistan that were committed by IRGC proxies al-Qaeda and the Taliban.

695. As a condition of its contract with the IRGC, including its Hezbollah Division and Qods Force, MTN promised to obtain embargoed U.S. technology to benefit the IRGC's, including the Qods Force's, terrorist enterprise.

696. Between 2009 and 2012, one or more purchasing agents working for the IRGC, including its Hezbollah Division and Qods Force, in the U.A.E. and elsewhere, spending money provided by MTN Group, and acting at the direction of MTN Group and its IRGC ally, collectively wired more than \$5,000,000 into the United States to associates in the U.S. who purchased embargoed technology for the IRGC's, including Hezbollah's and the Qods Force's benefit, which was then shipped from America to the U.A.E., where Hezbollah and the Qods Force assumed possession of the technology for use in its terrorist enterprise.

697. On information and belief, MTN and/or MTN's agents routed millions of dollars each year to its U.S. agents to pay for the embargoed dual-use U.S. technology it illegally obtained for the IRGC, including its Hezbollah Division and Qods Force, via transactions through the New York banking system, by causing money to be wired to MTN's U.S. agents to pay for MTN's U.S. agents to illegally obtain embargoed dual-use U.S. technology for the benefit of the Qods Force's terrorist enterprise.

vi. MTN Obtained Essential U.S. Services That Aided Hezbollah's, the Qods Force's, and Regular IRGC's Terrorist Capabilities

698. MTN's U.S. contacts were also key to its ability to obtain technical support from U.S. persons operating inside America, without which the IRGC, including its Hezbollah Division and Qods Force, could not have derived the terrorist benefits they did from MTN Irancell including the cash flow, network reliability, and enterprise computing benefits.

699. Between 2009 and 2012, and on information and belief ever since the mid-2000s, MTN Irancell relied upon one or more U.S. persons to service MTN Irancell's enterprise-level computers and associated networks, relying on one or more U.S. persons to maintain MTN Irancell's network remotely from the U.S. and, on at least one occasion, having such U.S. person travel to meet with MTN's Hezbollah and Qods Force allies in the U.A.E. to provide training to Hezbollah and the Qods Force. MTN, or agents acting at MTN's direction, sourced embargoed technology for the IRGC's, including Hezbollah' and the Qods Force's, benefit from, among others, Exit40, Akbari, Patco, MSAS, and TGO.

700. MTN routed millions of dollars each year to its U.S. agents, and sourced the sensitive dual-use U.S. technology, via transactions through the New York banking system, by causing money to be wired to MTN's U.S. agents to pay for MTN's U.S. agents to provide services, or obtain sensitive dual-use U.S. technology, for the benefit of the IRGC's, including the Qods Force's, terrorist enterprise.

701. On information and belief, MTN and/or MTN's agents routed millions of dollars each year to its U.S. agents in order to pay for the technology support services it illegally obtained for the IRGC, including its Hezbollah Division and Qods Force, via transactions through the New York banking system, by causing money to be wired to MTN's U.S. agents to

pay for MTN's U.S. agents to illegally provide technological support to maintain MTN Irancell for the benefit of the IRGC's, including the Qods Force's, terrorist enterprise.

G. The ZTE Defendants

1. ZTE Joined The Terrorist Conspiracy

i. Through Agreements With Hezbollah, Qods Force, And Regular IRGC Fronts Including But Not Limited To MTN Irancell, TCI, and Exit40, ZTE Agreed To Join A Company-Wide Conspiracy

702. MTN Group and ZTE Corp. followed the same IRGC playbook because they joined the same Conspiracy. *Reuters* concluded that "MTN was not alone" because "other foreign companies, including" "China's ZTE Corp, [] helped Iran undermine increasingly tougher sanctions." Stecklow, *How A Telecom Giant Got Round Sanctions On Iran*, *supra*.

703. ZTE and its subsidiaries, including ZTE USA and ZTE TX, joined the IRGC Conspiracy when ZTE, including ZTE USA and ZTE TX, agreed to provide U.S.-origin goods and services, in violation of U.S. sanctions, to TCI, while knowing that TCI was a front for Hezbollah the Qods Force, and Regular IRGC. ZTE's agreement to join the Conspiracy was in the form of contracts that ZTE signed with TCI and, on information and belief, MTN Irancell and MCI. The Conspiracy was adopted by ZTE's senior leadership and deployed throughout ZTE and its subsidiaries, including ZTE USA and ZTE TX.

704. ZTE and its subsidiaries, including ZTE USA and ZTE TX, furthered the IRGC Conspiracy when, on information and belief, ZTE and its subsidiaries, including ZTE USA and ZTE TX, agreed to provide U.S.-origin goods and services, in violation of U.S. sanctions, to Exit40, while knowing that Exit40 was a front for Hezbollah and the Qods Force. ZTE's furtherance of the Conspiracy was in the form of contracts that ZTE signed with Exit40 and, on information and belief, MTN Irancell and MCI. ZTE's furtherance of the Conspiracy through

Exit40 was adopted by ZTE's senior leadership and deployed throughout ZTE and its subsidiaries, including ZTE USA and ZTE TX. Plaintiffs' belief is based upon MTN Group's retention of Exit40, which, on information and belief, was for the same purpose and in response to the same IRGC instruction.

705. On information and belief, ZTE's contracts with its IRGC-front Iranian counterparties all included pledges to assist with the "security" of Iran.

ii. ZTE, ZTE USA, And ZTE TX Each Made Overt Acts In Furtherance Of The Conspiracy

706. Each of the ZTE Defendants, ZTE, ZTE USA, and ZTE TX acted in furtherance of the Conspiracy by, *inter alia*: (a) sourcing embargoed U.S.-origin technology useful to the terrorists for export to Hezbollah, the Qods Force, and Regular IRGC; (b) entering into contracts with U.S. suppliers to acquire the "essential" technology needed by the terrorists; (c) developing and using third-party companies to both conceal and facilitate its business with IRGC-front companies; (d) commingling U.S.-origin technology with non-U.S.-origin technology in order to evade detection of the illicit transactions scheme and Conspiracy; (e) lying to U.S. prosecutors and financial institutions regarding the nature of their activities in Iran and their true IRGC-front counterparties; (f) destroying evidence related to the illicit transfers and Conspiracy; and (g) moving one or more witnesses inside America who knew of the Conspiracy outside of United States jurisdiction. Each act described above was in furtherance of the Conspiracy.

2. ZTE Knowingly Assumed A Financial, Logistical, And Operational Role In Hezbollah's, The Qods Force's, And Regular IRGC's Terrorist Enterprise Against Americans Worldwide

707. ZTE bid on and secured contracts worth hundreds of millions of dollars to install cellular and landline network infrastructure in Iran. ZTE knew that its counterparties were IRGC, including Hezbollah and the Qods Force, fronts, operatives, or agents. ZTE thereafter

developed an elaborate system to fulfill those contracts using US-origin items, including dual-use goods controlled by the U.S. government due to their terrorism applications. ZTE did this in collaboration with, and with the assistance of, ZTE USA and ZTE TX.

i. ZTE Corp., ZTE USA, And ZTE TX Knowingly Facilitated MTN Irancell And TCI's Acquisition Of Embargoed American Technology, Logistical Support, And Technical Services, Which Flowed Through To The IRGC's Terrorist Proxies

708. Before 2011, ZTE sourced U.S. technology for Hezbollah, the Qods Force, and Regular IRGC. A Department of Justice Press Release dated March 7, 2017 (the "March 2017 Press Release") stated that ZTE violated U.S. sanctions by sending U.S.-origin items to Iran. It also announced ZTE's guilty plea to those charges and agreement to pay the U.S. government \$892,360,065. ZTE repeatedly violated export controls and illegally shipped U.S. technology to Iran, according to the March 2017 Press Release. On information and belief, ZTE did so in collaboration with and with the assistance of ZTE USA and ZTE TX.

709. ZTE's, ZTE USA's, and ZTE TX's (after its formation) company-wide scheme to obtain U.S.-origin goods and to evade export controls to get telecommunications technology into the hands of Hezbollah, the Qods Force, and Regular IRGC lasted from as early as 2010 to as late as 2016. While ZTE TX was not formed until at least 2013, Plaintiffs allege that ZTE TX and its employees participated in the scheme thereafter.

710. The cell phone technology and equipment ZTE sourced from inside the United States was subject to the embargo imposed and enforced by the United States Government. ZTE thus violated export controls designed to keep sensitive American technology out of the hands of IRGC, including Hezbollah and the Qods Force.

711. Through this scheme between January 2010 and January 2016 ZTE exported over 20 million U.S.-origin items to Hezbollah, the Qods Force, and Regular IRGC with a value of approximately \$32,000,000. ZTE did so without obtaining proper export licenses.

712. To evade the U.S. embargo, ZTE devised a scheme whereby an “isolation company” would be the vehicle used to hide ZTE’s shipment of prohibited U.S. technology to Hezbollah, the Qods Force, and Regular IRGC.

713. In early 2011, when ZTE determined that the use of its original “isolation company” was insufficient to hide ZTE’s connection to the illegal export of U.S.-origin goods to Hezbollah, the Qods Force, and Regular IRGC ZTE re-evaluated its strategy. In September 2011, four senior ZTE managers signed an Executive Memo which proposed that ZTE identify and establish new “isolation companies” that would be responsible for supplying U.S. component parts necessary for projects in embargoed countries.

714. After an international publication in March 2012 publicly revealed ZTE’s sale of prohibited equipment to Iran, ZTE temporarily stopped sending U.S. equipment to Hezbollah, the Qods Force, and Regular IRGC.

715. But in July 2014, ZTE began shipping U.S.-origin equipment to Hezbollah, the Qods Force, and Regular IRGC once again without the necessary licenses. Thus, properly understood, ZTE’s temporary pause was not the rumblings of a corporate conscience causing it to separate from terrorists but, rather, an effort to pause their support while they assessed whether they could get away with it. Once ZTE believed it could, on or about 2014, they resumed their support for Hezbollah, the Qods Force, and Regular IRGC.

716. ZTE made these additional shipments by using a new “isolation company.” In the new version of the scheme, ZTE purchased and manufactured all relevant equipment – both

U.S.-origin and ZTE-manufactured – and prepared them for pick-up at its warehouse by the new isolation company. The new isolation company then shipped all items to Hezbollah, the Qods Force, and Regular IRGC.

717. In the ZTE 2017 OFAC Settlement, ZTE, and its subsidiaries, including but not limited to ZTE USA and ZTE TX, admitted, in relevant part:

(i) From on or about January 2010 to on or about March 2016, ZTE, ZTE USA, and ZTE TX (starting on or after the date of its formation) together exported, sold, or supplied United States goods to Iran or the Government of Iran with knowledge that the goods were intended specifically for Iran or the Government of Iran and thereby evaded or avoided, attempted and/or conspired to violate, and/or caused violations of the prohibitions set forth in the ITSR.

(ii) ZTE, ZTE USA, and ZTE TX together engaged in at least 251 such transactions, and the total value of U.S.-origin goods in the 251 transactions constituting the apparent violations was \$39,622,972.

(iii) From approximately as early as November 2010 to approximately March 2016, ZTE's senior leadership developed and adopted a company-wide scheme (meaning ZTE USA and ZTE TX, starting on or after the date it was formed, were involved) to evade U.S. economic sanctions and export control laws.

(iv) ZTE's actions were developed and approved by the highest levels of its management and entailed the use of third-party companies to both conceal and facilitate its business with fronts for the IRGC, including its Hezbollah Division and the Qods Force.

(v) ZTE, ZTE USA, and ZTE TX together were “specifically aware of and considered the legal risks and consequences of violating U.S. economic sanctions and export control laws,” and were “specifically aware” of the potential consequences “if the U.S.

government learned of [ZTE]’s unauthorized reexportation of U.S.-origin goods to sanctioned countries, including Iran.”

(vi) Despite recognizing that “violations of U.S. law would be ‘inevitable’ if ZTE exported and/or reexported U.S.-origin goods to Iran,” ZTE, ZTE USA, and ZTE TX (starting on or after the date of its formation) together reexported and supplied a substantial volume of U.S.-origin goods to Iran from at least January 2010 to approximately March 2016 and “pursued and developed an evasive practice of ‘risk avoidance’ by utilizing isolation companies and other concealment activities” to do so.

(vii) ZTE’s contracts with Iranian companies from 2010 and 2012 required ZTE to export and/or reexport goods, services, and technology to Iran with the purpose of enhancing Iran’s telecommunications infrastructure, which in turn required supplying and/or attempting to supply Iran with U.S.-origin goods subject to the U.S. Department of Commerce’s Commerce Control List for anti-terrorism, national security, regional stability, and encryption item purposes and enhancing the law enforcement surveillance capabilities and features of Iran’s telecommunications facilities and infrastructure.

(viii) ZTE temporarily ceased performance of one of its contracts with an Iranian company [TCI], when *Reuters* reported in March 2012 that ZTE was circumventing U.S. sanctions law to provide U.S.-origin goods to TCI, but ZTE resumed its unlawful activity thereafter and “would not ultimately cease its unlawful activity or cooperate with the U.S. government until on or about March 2016.”

(ix) ZTE informed the U.S. government agencies and the public in 2012 that it was winding down its reexports of U.S.-origin goods to Iran. However, approximately one year later

in November 2013, ZTE resumed its unlawful business activities with Iran without updating or informing the U.S. government agencies of this change until on or about April 6, 2016.

(x) In connection with the decision to resume its business with fronts for the IRGC, including its Hezbollah Division and the Qods Force, in approximately November 2013, ZTE's highest-level leadership instituted directives authorizing various divisions of the company to surreptitiously resume business with those IRGC fronts, including by using a new third-party isolation company to conceal the resumption of prohibited activities from U.S. government investigators, the media, and others outside of ZTE.

(xi) ZTE USA and ZTE TX were directly implicated and directly participated in the scheme: (i) the ZTE 2017 OFAC Settlement Agreement, including its admissions of wrongdoing, was entered into by ZTE and its subsidiaries and affiliates, including ZTE USA and ZTE TX; (ii) the acts ZTE, ZTE USA and ZTE TX, agreed they had done included shipping embargoed items from the United States by commingling those items with foreign-made non-embargoed items; (iii) the conduct detailed therein as violations of the U.S. sanctions regime was done via activity within the United States, was described as a "company wide" scheme, and U.S.-origin goods were described as "essential," so on information and belief ZTE USA and ZTE TX participated directly in those activities; (iv) ZTE entered into contractual arrangements with U.S. suppliers, including Qualcomm and Broadcom, through and by ZTE USA, through which ZTE obtained the key technology for export to Iran; (v) an employee, on information and belief, of either ZTE USA or ZTE TX, was instructed by ZTE in China to leave the United States based on conduct done within the United States; (vi) ZTE has disclosed publicly that the same individual, Cheng Lixin, was simultaneously an officer of ZTE and the CEO of ZTE USA; and (vii) on information and belief the ZTE USA and ZTE TX were subject to multiple law

enforcement subpoenas and ZTE USA and ZTE TX facilities were searched by United States authorities related to wrongdoing done in the United States.

718. ZTE modernized telecommunications technology used by Iranian entities that were controlled by Hezbollah, the Qods Force, and Regular IRGC fronts, thereby pumping additional revenue into the coffers of Hezbollah, the Qods Force, and Regular IRGC and thereby the IRGC's proxies in Afghanistan, al-Qaeda and the Taliban.

719. ZTE, ZTE USA, and ZTE TX (after its formation) provided substantial banned technology to Iranian companies that were controlled by Hezbollah, the Qods Force, and Regular IRGC. Thereby, ZTE's illegally sourced technology ordinarily flowed through to IRGC proxies al-Qaeda and the Taliban. That banned technology was crucial to perpetrate terrorism. By way of example, terrorists were able to use cell phones and other telecommunication technology and software to perpetrate attacks on Americans.

720. ZTE also assisted the terrorist enterprise by serving as a long-term strategic partner for MTN Irancell, which was a front for Hezbollah, the Qods Force, and Regular IRGC.

721. It would be improper to characterize ZTE's role as only modernizing Iran's cellular and communications systems or providing cellular and landline telecommunications infrastructure for use by the Iranian population. On top of the millions of dollars that ZTE provided to the IRGC (including Hezbollah and the Qods Force) via TCI, ZTE also provided technical aid to the IRGC (including Hezbollah and the Qods Force) which facilitated terrorism. ZTE's, ZTE USA's, and ZTE TX's (after its formation) technology transfers were devastating to America's ability to protect Americans overseas from attacks committed by Iranian terrorist proxies like Hezbollah. This was because, as a result of their actions, the IRGC was in "a position to benefit from sensitive monitoring technology it can put to its advantage to enhance its

surveillance abilities,” which Hezbollah, the Qods Force, and Regular IRGC acquired after “ZTE Corporation sold TCI a powerful surveillance system capable of monitoring landline, mobile and internet communications.”²⁴² ZTE’s, ZTE USA’s, and ZTE TX’s (after its formation) technology transfer uniquely provided terrorists the ability to intimidate and coerce civilian populations.

722. For example, according to U.S. diplomatic cables and statements by Lebanese government officials, TCI and the Qods Force helped build Hezbollah’s fiber optic communication system, which was upgraded to include encrypted high-speed lines, and included, according to public reports and on information and belief, Defendants’ “Western technology.” This communication network facilitated intelligence collection and operations in Iraq, and helped Hezbollah defend against US intelligence collection. Hezbollah officials said that this network was their most valuable weapons system.²⁴³ TCI’s work in Lebanon, incorporating technology illegally smuggled by Defendants, enabled Hezbollah, the Qods Force, and Regular IRGC to fully integrate Hezbollah into its transnational command, control, communications, computing, intelligence, surveillance, and reconnaissance apparatus.²⁴⁴

723. Further, Iranian cellular networks, administered by ZTE and Huawei (for MTN), were also used to track and target U.S. forces in Afghanistan and Iraq. Because they included US technology, they could be used to locate U.S. forces with precision. U.S. soldiers close to the Iranian border would get continuously pinged by Iranian cell phone towers. The “ZXMT”

²⁴² Dr. Ottolenghi Sept. 17, 2015 Testimony.

²⁴³ Liz Sly, Lebanon's fiber-optic powder keg; Iran's hand seen in Hezbollah's growing communication grid, amid fears of 'state within a state,' *Chicago Tribune*, May 16, 2008.

²⁴⁴ Carl Anthony Wege, “Hizbollah–Syrian Intelligence Affairs: A Marriage of Convenience,” *Journal of Strategic Security*, Volume 4, Issue 3, 2011.

monitoring system that ZTE sold to Iran (with U.S.-origin components) could use this data to triangulate their positions and monitor their communications. Hezbollah, the Qods Force, and Regular IRGC also continuously upgraded Hezbollah's communications systems, enabling them to deploy cellular phones securely and thwarting U.S. efforts to collect intelligence on them.²⁴⁵

724. For a terrorist group intent on targeting Americans traveling in tightly secured convoys or on fortified bases, the technology that ZTE (via, on information and belief ZTE USA and ZTE TX) provided bolstered the terrorists' ability to conduct successful surveillance. The technology ZTE provided was vital to their ability to execute successful attacks, like the ones that killed and injured Plaintiffs and their loved ones. For these reasons, ZTE's acts, which allowed terrorists access to modern telecoms technology they could not otherwise obtain, facilitated intimidation, coercion, and violent acts and acts dangerous to human life.

725. The ample evidence of ZTE's own consciousness of guilt supports the inference that ZTE knew it was aiding Hezbollah, Qods Force and Regular IRGC-sponsored terrorism.

726. In 2017, the U.S. Commerce Department disclosed two internal ZTE documents discovered during its investigation. The first, from 2011 and signed by several senior ZTE executives, detailed the company's ongoing projects in Iran. Written by ZTE's general counsel, signed by its senior management, and flagged as "Top Secret," the document described a number of ways in which Defendants ZTE and its U.S. subsidiaries (including ZTE USA) were, in concert, violating U.S. laws well before 2011.²⁴⁶ In substance, it indicates that while high-level managers of ZTE were also directors of ZTE USA, and frequently shuttled between the two

²⁴⁵ Colin P. Clarke, "How Hezbollah Came to Dominate Information Warfare," *Jerusalem Post*, September 17, 2017.

²⁴⁶ ZTE "Report Regarding Comprehensive Reorganization and the Standardization of the Company Export Control Related Matters (Top Secret Internal Use Only)," August 5, 2011.

countries, their company's U.S. research centers — soon thereafter to be overseen by ZTE TX — were “often” engaged in the illegal transfer of U.S. research data to China. It also indicates that ZTE was illegally exporting US-origin technology as early as 2005, and that ZTE, as well as its officers, knew that they could face both criminal and civil penalties based on their existing contracts. The second document laid out in a complex flow chart ZTE's proposed method for circumventing United States export controls and getting U.S.-origin technology to Iran.

727. According to the then-Acting Assistant Attorney General, Mary B. McCord, “ZTE engaged in an elaborate scheme to acquire U.S.-origin items, send the items to Iran and mask its involvement in those exports,” and the plea agreement ZTE signed “alleges that the highest levels of management within the company approved the scheme.”

728. In 2012, after ZTE's original contract with TCI, which allowed the IRGC (including Hezbollah and the Qods Force) to build a country-wide surveillance system capable of monitoring landline, mobile, and internet communications, was widely reported, ZTE claimed it would stop its business with fronts for the IRGC. In or around March 2012, ZTE spokesman David Shu said in a telephone interview “[w]e are going to curtail our business in Iran.” Although that was a lie, because ZTE thereafter doubled-down on its business relationships with Hezbollah, the Qods Force, and Regular IRGC fronts, it was also an admission that such business was fraught with risk that it would support and contribute to terrorism.

729. Ashley Yablon, ZTE USA's former general counsel, gave the FBI an affidavit in May 2012 alleging ZTE had plotted to cover up the Iran sales. ZTE employees asked Mr. Yablon, a ZTE USA employee, to develop a strategy to transfer U.S.-origin goods to sanctioned countries. Yablon has indicated that during the U.S. investigation into ZTE's transfer of U.S.-origin technology to Iran, ZTE internally discussed destroying evidence, and it has been reported

that ZTE employees told Mr. Yablon to gather the evidence of the U.S.-origin technology transfers to Iran, which he had in the United States, and Mr. Yablon instructed ZTE USA employees not to destroy evidence regarding ZTE USA's exports relevant to ZTE's agreement to export U.S.-origin goods. After Yablon's affidavit became public in July 2012, ZTE, which otherwise directed his activities in the United States, placed Yablon on administrative leave.

730. ZTE destroyed evidence of its business with fronts for Hezbollah, the Qods Force, and Regular IRGC and, on information and belief, ZTE USA destroyed evidence in the United States of its business with fronts for Hezbollah, the Qods Force, and Regular IRGC.

731. There has been public reporting related to ZTE's internal documentation of its strategies for how to get around export controls so it can do business with state sponsors of terrorism. Those strategies included using a codeword for Iran in internal documents. On information and belief ZTE USA and/or ZTE TX participated in these strategies.

732. Throughout the scheme, ZTE attempted to conceal its export of U.S.-sourced technology to Hezbollah, the Qods Force, and Regular IRGC by, among other things, requiring its employees to sign non-disclosure agreements, lying to its own lawyers regarding its exports, lying to a forensic expert hired to conduct an internal investigation, and adopting a policy and hiring thirteen (13) employees to alter, delete, and hide data relevant to the export sales.

733. ZTE admitted that it assembled a team of IT employees to alter, process, sanitize, and/or remove references to Iran in ZTE's internal databases regarding its business with fronts for the IRGC. The IT team coordinated with various divisions throughout the company, including the sales, procurement, and finance divisions, as well as ZTE's subsidiaries in the United States including but not limited to ZTE USA, to locate and remove any references to Iran

or ZTE's business with IRGC fronts. The employees executing this IT project were instructed to, and did, delete their emails related to the project.

734. ZTE's acts related to its export of U.S. embargoed technology to Iran, and its attempts to hide and obscure the same, were labelled by the U.S. Government as a "cover-up."

735. In relation to ZTE's acts to export U.S. embargoed technology to Iran, and its attempts to hide and obscure the same, the U.S. Government charged ZTE with making materially false, fictitious, and fraudulent statements and representations to the FBI.

736. In 2017, ZTE chairman and chief executive acknowledged guilt for its acts to evade the embargo and provide banned technology and goods to Iran, saying "ZTE acknowledges the mistakes it made [and] takes responsibility for them."

737. ZTE knew that it was breaking U.S. law when it exported sensitive telecommunications technology to Hezbollah, the Qods Force, and Regular IRGC and knew or recklessly disregarded that the entities with which it was transacting business (and indeed who were receiving that technology) were fronts for Hezbollah, Qods Force, and Regular IRGC terrorists who were actively attempting to kill Americans by facilitating attacks by al-Qaeda and the Taliban against Americans in Afghanistan.

738. From 2008 through at least 2016, ZTE's illicit transactions with MTN Irancell, the Bonyad Mostazafan, IEI, TCI, and/or the Akbari Fronts, provided millions, annually, in illicit funds, weapons, and operational support to Hezbollah, the Qods Force, and Regular IRGC, which flowed to al-Qaeda and the Taliban and was used to attack Americans in Afghanistan, including Plaintiffs and their loved ones.

ii. ZTE Corp., ZTE USA, And ZTE TX Substantially Increased MTN Irancell And TCI Revenue By Illicitly Sourcing Embargoed American Technology, Logistical Support, And

Technical Services, Which Flowed Through To The IRGC's Terrorist Proxies

739. ZTE Corp.'s ZTE USA's, and ZTE TX's illicit transactions with MTN Irancell, the Bonyad Mostazafan, IEI, TCI (including MCI), Exit40, and/or the Akbari Fronts, provided millions, annually, in illicit funds, weapons, and operational support to, among others, Hezbollah, the Qods Force, and Regular IRGC, which flowed through to al-Qaeda and the Taliban and facilitated attacks against Americans in Afghanistan, including Plaintiffs.

740. ZTE Corp., ZTE USA, and ZTE TX significantly increased the cash flowing through MTN Irancell and TCI, and ultimately being deployed by Hezbollah, the Qods Force, and Regular IRGC. They did so by illicitly supplying the state-of-the-art American technologies, like servers, to MTN Irancell and TCI, and by extension the IRGC (including Hezbollah and the Qods Force) needed to attack Americans abroad.

iii. ZTE Corp., ZTE USA, And ZTE TX Routed Bribes To The Key Procurement Decisionmakers At MTN Irancell And TCI, Which Flowed Through To The IRGC's Terrorist Proxies

741. ZTE Corp. has engaged in serial bribery around the world to win business including large 6- and 7-figure bribes. According to a report published by a team of investigators hired by a hedge fund, "ZTE has engaged in systemic, centrally managed corruption at a scale rarely seen in international commerce."²⁴⁷

742. On at least two prior occasions, the same ZTE Corp. leadership team here bribed foreign officials in procurement settings that were like MTN Irancell (other than being in a

²⁴⁷ Bill Gertz, *Report Urges U.S. Action Against Chinese Telecom Giant ZTE Over Corruption Record*, Wash. Times (Dec. 10, 2020) ("Gertz, *Report Urges U.S. Action*").

different geography). ZTE Corp. paid nearly \$800,000 to one decision-maker, more than \$1 million to a second, and \$10 million to a third (all serving in different countries).²⁴⁸

743. On March 13, 2020, NBC News reported that “ZTE” was “the subject of a new and separate bribery investigation by the Justice Department,” under the Foreign Corrupt Practices Act (“FCPA”). The investigation “center[ed] on possible bribes ZTE paid to foreign officials to gain advantages in its worldwide operations.”²⁴⁹

744. The Justice Department’s current FCPA investigation concerning ZTE Corp. involves ZTE Corp.’s conduct within the United States.²⁵⁰

745. ZTE is not a “normal” multinational corporation, but a notoriously dirty company that seeks to advance the agenda of the Chinese Communist Party. It is willing to engage in corrupt deals that most other corporations shun. For example, NBC News noted that “Norway’s giant government pension fund banned ZTE from its investment universe” in 2016 “based on

²⁴⁸ Don Woolford, *Somare, The Controversial Father of PNG*, AAP Newswire (Febr. 25, 2021) (“[Michael Somare] faced various claims of impropriety or worse, including being given a \$780,000 bribe by Chinese phone giant ZTE. He was found guilty of submitting late and incomplete financial statements.”).

²⁴⁹ Gretchen Morgenson and Tom Winter, *The U.S. Is Now investigating Chinese Telecom Giant ZTE For Alleged Bribery*, NBC News (Mar. 13, 2020) (“Morgenson and Winter, U.S. Is Now Investigating”).

²⁵⁰ This is necessarily true because, as the *Wall Street Journal* reported, “[t]he U.S. usually doesn’t have jurisdiction to enforce the FCPA against foreign companies lacking securities that trade in the U.S., but can investigate such cases if actions took place within its borders, or if money used in the alleged scheme was wired through the nation’s financial system.” Aruna Viswanatha and Corinne Ramey, *U.S. Probes Chinese Telecom Giant ZTE for Possible Bribery; The Justice Department Investigation Comes After The Company Already Pleaded Guilty To Dodging U.S. Sanctions On Iran*, *Wall Street Journal* (Mar. 13, 2020).

‘the risk of severe corruption.’”²⁵¹ As *NBC News* stated, “[o]nly three other companies are barred by the Norwegians for ‘gross corruption’ alongside ZTE.”²⁵²

746. ZTE Corp. has pursued an integrated global sales strategy, under which one may infer that ZTE Corp. followed the same, or a substantially similar, bribery tradecraft with respect to similar “pitches” for other state-owned telecom companies.

747. Plaintiffs’ allegations comport with ZTE Corp.’s kickback schemes in other similarly situated governments, e.g., the Philippines, where ZTE Corp. paid millions in bribes.²⁵³

748. Audrye Wong is an Assistant Professor of Political Science and International Relations at USC and a Wilson Center China Fellow. In 2021, Ms. Wong published a detailed analysis of Chinese economic tradecraft including, among other things, the Chinese Communist Party’s heavy emphasis on bribery as a matter of policy:

But perhaps *the most prominent feature of China's economic statecraft* is its use of *positive inducements*. These incentives come in two forms: under the table, whereby Beijing buys off political leaders through illicit deals, and by the book. ... China often provides economic inducements in illicit and opaque ways ... As Chinese companies have increasingly invested overseas, state-owned enterprises or private companies, sometimes with the tacit approval of Chinese officials, have offered bribes and kickbacks to elites in countries receiving investment or aid projects in order to grease the wheels of bureaucracy. At other times, Chinese companies have bypassed the process of competitive bidding and regulatory approval to secure a contract, often at inflated costs, generating extra profits for both Chinese actors and local elites. I call such inducements "subversive carrots." In many ways, their use reflects China's domestic political economy, where businesses depend on official connections, corruption is widespread, and few regulations govern foreign investment and foreign aid. My research shows that this method works *best* in countries that also have *little public accountability*-

²⁵¹ *Id.*

²⁵² *Id.*

²⁵³ See, e.g., Audrye Wong, *How Not to Win Allies and Influence Geopolitics: China's Self-Defeating Economic Statecraft*, Foreign Affairs, Volume 100; Issue 3 (May 1, 2021), (emphasis added), 2021 WLNR 15954005.

where the flow of information is restricted, and political leaders need not worry about public opinion and the rule of law.²⁵⁴

749. On information and belief, from 2010 through 2016, ZTE Corp. caused the payment of at least several million dollars, denominated in U.S. Dollars, to one or more officers, agents, or directors of MTN Irancell, TCI, and/or MCI. This money flowed through to fund and arm the IRGC's Shiite Terrorist Proxies and the IRGC's Sunni Terrorist Proxies to support their attacks against Americans around the world.

3. ZTE Knowingly Assumed A Financial, Logistical, And Operational Role In The Taliban's, Including The Haqqani Network's, Terrorist Enterprise In Afghanistan, Directly And Indirectly Financing And Arming IRGC Proxy Attacks In Afghanistan And Iraq

750. ZTE operated lucrative businesses in post-invasion Afghanistan by servicing a broad array of customers there. To increase their profit margins by redirecting attacks away from their business interests – and to intentionally assist the Taliban's effort to drive Americans out of Afghanistan – ZTE knowingly paid protection money to the Taliban, including its Haqqani Network. When ZTE did so, ZTE knowingly assumed a financial, logistical, and operational role in the Taliban's, including the Haqqani Network's, terrorist enterprise in Afghanistan and beyond by directly and indirectly routing protection payments to these terrorists in cash and “free goods,” including secure American cell phones.

751. ZTE has become one of the world's most valuable communications technology manufacturers by providing a comprehensive suite of communications technologies services to customers in high-risk geographies from a counter-terrorism perspective, including geographies where Hezbollah, the Qods Force, and Regular IRGC and IRGC proxies al-Qaeda and the

²⁵⁴ Audrye Wong, *How Not to Win Allies and Influence Geopolitics: China's Self-Defeating Economic Statecraft*, Foreign Affairs, Volume 100; Issue 3 (May 1, 2021), (emphasis added), 2021 WLNR 15954005.

Taliban, raised and moved money to facilitate terrorist attacks through protection payments, procurement corruption, “free goods” payoffs, payments routed through consultants, and similar schemes that depended upon complicit corporate partners. ZTE followed that model in Afghanistan, where ZTE continuously operated for decades.

752. From 2006 through 2019, ZTE sold products to Afghan telecommunications operators, e.g., MTN Afghanistan, which was MTN’s subsidiary in Afghanistan, which were manufactured by the ZTE Defendants.

753. While ZTE was achieving rapid growth in Afghanistan, the communications sector provided a critical source of financing for the Taliban, in the same manner as it did for Defendants Huawei and MTN. ZTE’s payments mirrored the protection money delivered by Huawei and MTN. Just as the Taliban raised “taxes” from international contractors doing business in Afghanistan, so too did it levy similar “taxes” on “the big telecom companies” like ZTE.²⁵⁵

754. ZTE’s services in Afghanistan required ZTE work in areas that were controlled or contested by the Taliban, in which ZTE paid protection payments as a cost of doing business.

755. ZTE’s sales to its Afghan customers depended upon ZTE personnel successfully driving large truck convoys containing ZTE’s lucrative Afghan-customer-bound goods through Taliban, including Haqqani Network, controlled or contested geographies in Pakistan and Afghanistan.

756. ZTE paid the money as protection: ZTE decided that the cheapest way to shield their projects from attack was to pay the Taliban to leave them alone and instead attack other targets – like Plaintiffs and their family members. Similar payments were pervasive throughout

²⁵⁵ *Ruttig, The Other Side* at 20.

Afghanistan and supplied the Taliban with an important stream of financing to fund their terrorist attacks across the country.

757. The Taliban conveyed its protection-money demands to ZTE via Night Letters similar the ones the Taliban sent to MTN and Huawei.

758. ZTE was a particularly aggressive practitioner of protection payments. Rather than invest in expensive security for shipments, ZTE purchased cheaper “security” by buying it from the Taliban, including its post-FTO-designation Haqqani Network.

759. ZTE negotiated its protection payments in direct discussions between ZTE Afghanistan’s security department and Taliban, including Haqqani Network, commanders.

760. Like other contractors in Afghanistan, ZTE generally paid, as protection to the Taliban (including its Haqqani Network), at least ten percent (10%) of its contract budget – and, on information and belief, much more than this – on any contract in which ZTE, including any ZTE affiliate or contractor, provided services to any customer in Afghanistan, since the Taliban controlled or contested every geography in which ZTE worked.

761. ZTE’s practice of making protection payments to the Taliban extended to the Haqqani Network. From at least 2008 through 2017, ZTE operated infrastructure projects sites, and/or sold communications technology products to customers (and therefore transported lucrative commodities through territory) in Afghanistan that was controlled by the Haqqani Network, and ZTE purchased security for those project sites and shipments by paying the Haqqani Network. The Haqqani Network’s chief financial operative, Nasiruddin Haqqani, oversaw those payments, and they typically occurred on a semi-annual basis, and the Haqqani Network’s overall involvement in the scheme was ultimately supervised by Sirajuddin Haqqani, who was at all times a dual-hatted al-Qaeda/Taliban terrorist.

762. ZTE Corporation keyed ZTE's rapid growth in Afghanistan by sponsoring a vast stream of payoffs to the Haqqani Network from 2006 through today, which flowed through to benefit al-Qaeda and the entire Taliban. Under Sirajuddin Haqqani's leadership, as executed by his immediate family members, the Haqqani Network was responsible for collecting "taxes" from Afghanistan's telecom companies, which were the single largest (legal) industry and tax base in Afghanistan – and thus a key source of funding and power for the Taliban and al-Qaeda, both of which were effectively led by Sirajuddin Haqqani in Afghanistan and Pakistan.

763. The logic behind ZTE's payoffs to the Haqqani Network matched the logic motivating ZTE's joint venture with the IRGC. ZTE's leadership intended to harm American interests in Afghanistan (like Iraq), and supporting the Taliban allowed them to do so. ZTE's decision to route monthly protection payments to al-Qaeda (via Sirajuddin Haqqani and his immediate family members) and the Taliban was made so that ZTE would not face the risk that terrorists commanded by Sirajuddin Haqqani would destroy some of ZTE's shipments. The going protection payment rate was usually around \$500 to \$2,000 per truck per convoy. In some areas, ZTE caused payments to be made to local Taliban, including Haqqani Network, commanders. In other places, where ZTE operated in a Taliban-controlled environment, the payments would be sent to the Taliban's Quetta Shura for southern Afghanistan, e.g., Helmand, or the Taliban's Miram Shah Shura for eastern Afghanistan, e.g., Paktia (Sirajuddin was involved in the former and led the latter).

764. By 2006, the Taliban prized the acquisition of Western communications technologies, including American-made cell phones, that were "washed" through the IRGC or one of its corporate partners, like ZTE.

765. From 2006 through 2021, ZTE also made protection payments to the Taliban, including its Haqqani Network, in the form of “free goods” – in particular, free communications technologies like cell phones – as an alternative to paying the terrorists in cash. When ZTE did so, ZTE directly provided to the Taliban, including its Haqqani Network, a broad range of communications technologies including, but not limited to, American mobile phones such as American-made Motorola phones, which ZTE reached into the U.S. to specifically acquire for the purpose of transferring such technologies to the IRGC and its proxies, including the Taliban.

766. On information and belief, ZTE transferred millions of U.S. Dollars’ worth of American communications technologies, including more than a thousand (1,000) “free goods” black market American-made cell phones to the Taliban, including its Haqqani Network, which ZTE acquired from the U.S. and delivered to the Taliban, each year from 2006 through 2021.

767. ZTE’s transfer of free, and illicitly sourced, communications technologies, including technologies that ZTE sourced from the United States, as a means to bribe the Taliban, including its Haqqani Network, comports with ZTE’s long-standing embrace of “free goods” as a core, decades-long, global strategy to route bribes to recipients.

768. U.S. military and intelligence officials have publicly confirmed Plaintiffs’ allegations against ZTE. For example, on June 8, 2012, *Business Insider* confirmed – citing American “military sources” and “former and current intelligence sources” – that that “China [was] likely to remain an aggressive and capable collector of sensitive U.S. economic information and technologies.”²⁵⁶ Thus, “[a]nother concern raised by [U.S. military] sources

²⁵⁶ *Business Insider, Military Sources: China Could Shut Down All The Telecommunications Technology It Sold To America* (June 8, 2012) (“Business Insider”).

[was] that Huawei and the other Chinese telecommunications companies [i.e., ZTE] also provide[d] technology to Iran and the Taliban.”²⁵⁷

769. When ZTE provided free communications technologies to the Taliban, including black market American cell phones, ZTE provided the terrorists a cash equivalent that sponsored tremendous violence. At a going rate of \$2,000 per black market cell phone, for example, the value of ZTE’s illicit phones supplied to the Taliban, delivered at least \$2 million per year in value to the Taliban, including its Haqqani Network.

770. When ZTE acquired and transferred free communications technologies to the Taliban, including black market American cell phones, from the United States and delivered such technologies to the Taliban, including its Haqqani Network, ZTE provided devastating operational and logistical assistance to the Syndicate in addition to the financial value of such goods through the same operational and logistical benefits that such black market communications technologies, including American cell phones, accorded to terrorists worldwide.

771. ZTE also directly aided al-Qaeda when ZTE transferred cash and free goods, including the above-described communications technologies and black market American cell phones, to the Haqqani Network because Sirajuddin Haqqani and his immediate family members, who were responsible for collecting protection payments from telecom companies like ZTE, were also members of al-Qaeda, and thus ZTE funded and logistically supplied al-Qaeda when ZTE routed cash and free goods protection payments to the Haqqani family.

772. ZTE’s overall payments to the Taliban, including its Haqqani Network, reached millions of dollars in value in cash and “free goods” payments of communications technologies, including black market U.S. cell phones each year from 2006 through the present. At that rate,

²⁵⁷ *Id.*

the ZTE Defendants caused at least tens of millions in U.S. Dollar-value in cash and “free goods” to flow through to the Taliban, from 2006 through the present, which furthered the IRGC Conspiracy and directly aided the IRGC proxies who committed such attacks, i.e., al-Qaeda and the Taliban, through attacks committed by joint al-Qaeda/Taliban cells and/or by the Taliban that were planned and authorized by al-Qaeda.

4. ZTE’s Assistance To Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, And The Taliban, Comports With ZTE’s Historical Business Practices In International Markets

773. Like MTN, ZTE’s conduct reflected a willingness to support America’s enemies, and engage in illicit financial transactions, as a way to increase profits in Iran. The same calculation pervaded ZTE’s other conduct throughout the world. ZTE’s other conduct further demonstrates its pattern and practice of transacting with violent actors to increase ZTE revenue.

774. ZTE has been called a “poster child” for sales of Chinese made network equipment at low prices that “allow the Chinese government to eavesdrop on all communications running on their equipment.”²⁵⁸

775. Like Iran, North Korea is a designated state sponsor of terrorism with a long history of attacking and murdering Americans overseas. ZTE’s illicit transactions concerning North Korea, therefore, further inform ZTE’s deliberate support for terror.

776. ZTE had a long-term relationship with North Korea. A 2020 civil forfeiture action revealed that — based on ZTE’s disclosures to the U.S. government — it had dedicated account executives and a physical presence in North Korea no later than 2005 and 2007, respectively. ZTE tasked its North Korea account manager with creating two shell companies, one to receive North Korean payments in dollars, and the other to transfer the money — often

²⁵⁸ Gertz, *Report Urges U.S. Action*.

using the U.S. financial system — to ZTE. The value of the goods smuggled this way exceeded \$300 million. During this time, North Korea had an extensive relationship with Hezbollah, the Qods Force, and Regular IRGC and Hezbollah. One court found this support included providing military hardware and training, most notably training for senior leaders and Hezbollah’s intelligence cadre. Thereby, North Korea provided material support to Hezbollah, including but not limited to in relation to the illicit technology transferred to North Korea by ZTE.

777. As part of its guilty plea, “ZTE ... pleaded guilty ... to violating U.S. sanctions against Iran and North Korea.”²⁵⁹ Like with Iran, when it helped North Korea source embargoed goods, ZTE knew or recklessly disregarded that it was engaging in illicit transactions with North Korean counterparties in violation of U.S. and international sanctions that were designed to choke off North Korea’s support for terrorism. Moreover, even after ZTE got caught helping North Korea evade U.S. sanctions (and pledged to be truthful with the U.S. government), ZTE lied and made additional false statements to American authorities.²⁶⁰

²⁵⁹ Gretchen Morgenson and Tom Winter, *The U.S. Is Now investigating Chinese Telecom Giant ZTE For Alleged Bribery*, NBC News (Mar. 13, 2020) (“Morgenson and Winter, *U.S. Is Now Investigating*”).

²⁶⁰ As *NBC News* noted, “[i]n the deal with the U.S. government [in 2017], ZTE also agreed to a denial of export privileges that could be activated for seven years if the company committed additional violations. In mid-April 2018, the Commerce Department activated the denial of privileges after determining that ZTE had made false statements to the government about actions it had taken to punish employees involved in the Iran and North Korea activities. While ZTE said it had reprimanded the employees, the government later found that the company had rewarded them with bonuses. Activating the denial meant that ZTE could not buy semiconductors required for its products.” *Id.*

778. As legal commentator Stewart Baker noted at the time in 2012, when discussing ZTE's corporate criminal culture, that "[a] kind of perfect storm has struck ZTE, ... [a] storm largely of ZTE's own making."²⁶¹ He explained:

ZTE ... ha[s] been the subject[] of great national security concern for years. ... Now, though, the mess is everywhere, and the House intelligence investigation will surely be heavily influenced by the new evidence that ZTE at least is quite capable of carrying out sophisticated telecommunications surveillance, of violating US law, and perhaps even lying about it later. Which, come to think of it, is pretty much what US intelligence agencies have been saying all along.²⁶²

779. Plaintiffs' allegations concerning ZTE's willingness to pay bribes and protection payments, in cash and free goods, are also consistent with ZTE's recent history, as documented by press reports concerning allegations of "rampant corruption" and programmatic bribery by ZTE around the world for decades.²⁶³

5. ZTE's Assistance To Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, And The Taliban Had A Substantial Nexus To The U.S.

780. ZTE's assistance to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, relied on significant contacts with the United States. As it has admitted, ZTE orchestrated both those U.S. contacts and ZTE's violation of U.S. law, including, on information and belief, by and through coordination with ZTE USA and ZTE TX. Like MTN, ZTE employs a top-down management structure in which ZTE centralizes operational control over the functions performed by its various subsidiaries.

²⁶¹ Stewart Baker, *And You Think You're Having A Bad Day?*, The Volokh Conspiracy (July 13, 2012) (emphasis added), 2012 WLNR 14621514.

²⁶² *Id.*

²⁶³ See, e.g., Gertz, *Report Urges U.S. Action* ("Chinese telecommunications company ZTE has been involved in international bribery incidents around the world but so far escaped prosecution by the Justice Department for corrupt practices... according to a report... based on court documents, interviews with prosecutors, and news reports showing ZTE linked to corrupt practices in more than a dozen countries....").

781. ZTE's decision to assist Hezbollah, the Qods Force, and Regular IRGC and by extension their proxies, al-Qaeda and the Taliban, had a substantial nexus to the United States for the reasons explained below.

i. ZTE's Conduct Targeted the United States

782. ZTE's provision of material support to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, was expressly aimed at the United States. At all relevant times, ZTE knew that Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, were targeting the United States. Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, did not conduct an indiscriminate terrorist campaign that merely injured Americans by chance. Instead, Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, directed attacks at *Americans* with the specific intent of killing *Americans* in particular – so that they could inflict pain in the United States and influence U.S. policy. Hezbollah's, the Qods Force's, Regular IRGC's, al-Qaeda's, and the Taliban's, including its Haqqani Network's, ultimate, shared, publicly stated goal was to effect a withdrawal of American forces from Afghanistan and the broader Middle East. Each terrorist attack that killed and injured Plaintiffs was part of that campaign of anti-American terrorism.

783. ZTE's decision to reach into the United States, including by coordinating with ZTE USA and ZTE TX, to obtain embargoed dual-use technology to aid the IRGC's, including Hezbollah's and the Qods Force's, terrorist enterprise was also expressly aimed at the United States. Like MTN, ZTE knew, based on conversations with IRGC, including Hezbollah and the Qods Force, agents, that Hezbollah, the Qods Force, and Regular IRGC viewed ZTE's assistance as vital to Iranian national "security," which ZTE understood to inherently involve the promotion of terrorist violence against Americans worldwide as part of Hezbollah's, the Qods Force's, and Regular IRGC's effort to export its Islamic Revolution and drive the U.S. out of Afghanistan.

784. On information and belief, like MTN, ZTE also knew, based on conversations with U.S. officials, that it was assuming an active role in a Hezbollah, the Qods Force, and Regular IRGC plot to develop cash flow and source vital dual-use components for Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban. ZTE further knew of the critical importance that communications and computing technology plays for terrorists.

785. When ZTE, ZTE USA, and ZTE TX sourced embargoed technology, including by coordinating with ZTE USA and ZTE TX, that the United States had publicly declared could benefit IRGC, including Hezbollah and the Qods Force, efforts to kill Americans, they intentionally helped arm terrorists they knew were targeting the United States. On information and belief, Hezbollah, the Qods Force, and Regular IRGC made ZTE agree to a similar contractual pledge as the one in which MTN agreed to aid Iran's "defensive, security, and political" interests outside of Iran. On information and belief, at all times, ZTE knew or recklessly disregarded that "security" was a euphemism for IRGC, including Hezbollah and the Qods Force, terrorist operations outside of the territorial borders of Iran. When ZTE, ZTE USA, and ZTE TX obtained the technology requested by its IRGC, including Hezbollah and the Qods Force, partners, each took actions in the United States and targeted at United States by helping the terrorists improve their bombs, rockets, communications, and intelligence gathering.

786. Although ZTE's primary motivation for assisting Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and Taliban was financial, ZTE also intended to harm Americans in Afghanistan. One reason ZTE cooperated with Hezbollah, the Qods Force, and Regular IRGC was to align itself with their effort to drive Americans out of Afghanistan.

787. Like MTN, ZTE intended to harm Americans because it decided that was the necessary price of maintaining a good relationship with Hezbollah, the Qods Force, and Regular

IRGC who were explicit, that they expected their partners to provide significant help in fighting against U.S. forces in particular. Thus, for ZTE to achieve its business objectives vis-à-vis Hezbollah, the Qods Force, and Regular IRGC fronts who controlled TCI and MTN Irancell – both of which ZTE serviced – ZTE needed to disassociate itself from the United States and prove that it could deliver value to the IRGC’s terrorist campaign against U.S. forces in Afghanistan.

788. On information and belief, like MTN’s, ZTE’s agreement to aid Hezbollah, the Qods Force, and Regular IRGC fulfilled an obligation by ZTE to engage in “defensive, security and political cooperation” with its IRGC, including Hezbollah and Qods Force, counterparties.²⁶⁴

789. Indeed, ZTE’s contract with TCI, according to Yablon, obligated ZTE to transfer its U.S.-built surveillance systems to TCI. When *Reuters* revealed that the ZXMT system contained U.S.-origin components, the Department of Commerce, BIS, served ZTE USA with an administrative subpoena and the U.S. Attorney’s office for the Northern District of Texas opened its grand jury investigation and the FBI served ZTE USA with criminal subpoenas.

790. The “surveillance function” built into ZTE’s contract, on information and belief, obligated ZTE to collaborate with Iranian ‘security’ authorities, including, *inter alia*, IRGC entities that implemented the regime’s campaign of terrorism.

791. Thereby ZTE, along with IRGC-controlled TCI, are responsible for helping the IRGC collect signals intelligence within Iran. Per the U.S. government, the IRGC Committee to Determine Instances of Criminal Content identifies websites, which TCI blocks and monitors.

792. In their campaign of mass repression, these IRGC, including Hezbollah and the Qods Force, agencies rely on technology illegally supplied by the Defendants, and, to justify their actions, a law which criminalizes any effort to evade the IRGC’s censorship, creating online

²⁶⁴ Exhibit A, MTN Group-Irancell Consortium Letter Agreement § 8.

“groups or gatherings” that threaten the state, or linking to sites connected to “wayward and illegal groups and movements” as “creating content against national security.”²⁶⁵

793. *First*, ZTE’s support for Hezbollah, the Qods Force, and Regular IRGC did not merely grow ZTE’s profits by allowing it to obtain lucrative business from MTN Irancell and TCI in the first instance; it also benefited ZTE’s business by inflicting harm on an enemy (the United States) of one of ZTE’s most important business partners (Hezbollah, the Qods Force, and Regular IRGC) in order for ZTE to curry Iranian favor to gain market share for a potentially uniquely lucrative telecom and communications market (Iran).

794. *Second*, ZTE’s support for attacks against U.S. citizens by Shiite terrorists advanced the foreign-policy interests of ZTE’s most important business partner: the Chinese Communist Party (or “CCP”).

795. At all relevant times, ZTE has acted as an anti-American Chinese nationalist company that actively seeks to advance the interests of the Chinese Communist Party.

796. ZTE specifically pursued transactions with Qods Force fronts in order to harm the United States in the Middle East as part of a broader Chinese Communist Party strategy to inflict pain on America in the Middle East by supporting the Qods Force and its terrorist campaign against Americans there.

797. Indeed, ZTE has pursued this objective continuously since 9/11. For example, less than two weeks after that attack, commentators were already observing ZTE’s efforts to curry favor with the Taliban, even though they were understood to have sheltered bin Laden and contributed to the attack as a result. As one wrote at the time:

China ... has been playing its own complex “Great Game,” through the Taliban in Afghanistan, and in alliance with Pakistan. ...

²⁶⁵ Justice for Iran, *Gerdab: a Dictated Scenario*, at 36 (2012), <https://tinyurl.com/4a8hfps9>.

The Chinese attitude towards radical “Islamism” is two-faced. Beijing is happy to train and send armed insurgents – separatist terrorists -- to ... sow mischief wherever it can against Western interests. But it is also worried, sometimes to the point of paranoia, about the security threat to its own Uighur territory. ...

From the Beijing point of view, co-operation with the Taliban kills two birds with one stone. On the one hand, China has been helping to nurture a very painful thorn in the West’s backside; on the other, it is buying off Taliban encouragement for Uighur separatists. Until Sept. 11, it appeared Beijing’s prospects in Kabul were win-win.

By coincidence or otherwise, on Sept. 10, the day before the organized terror assault on New York City and Washington D.C., Chinese representatives in Kabul signed a memorandum of understanding for economic and technical co-operation with Mullah Mohammed Ishaq, the Taliban minister for mining.

It was the most comprehensive of a series of contractual agreements between Beijing and the Taliban, in defiance of the spirit if not the letter of both Western and United Nations sanctions. It confirmed the Chinese role as the Taliban’s best friend outside the Islamic world.

The most interesting part of the agreement is a promise to build desperately needed infrastructure for the Taliban regime, throughout the 90 per cent of Afghanistan's surface area now under Taliban control.

Already, last year, two Chinese telecommunications firms, Huawei Technologies and ZTE, began work laying secure land-based phone lines between and within Kabul and Kandahar, and they may well be directly involved in providing communications services to the terrorist "underground" (literally, for it works from caves) in the Kandahar region.

Huawei is the firm that has been installing communications equipment for Iraq's air-defence system. It was named in a protest to the Chinese government by the Bush administration on its first day in office.

The aid to Afghanistan is by no means confined to economy and infrastructure. Political contacts between China and the Taliban have been increasing rapidly. ...

China tries to help the Afghan terrorist regime in its struggle against the West[.]²⁶⁶

²⁶⁶ David Warren, *How China Advances Its Imperial Ambitions By Backing The Taliban*, Ottawa Citizen (Canada), (Sept. 22, 2001), 2001 WLNR 6660411.

798. Faithful to its Chinese Communist Party-supporting trade efforts, ZTE always pursued the CCP's nationalistic Chinese agenda. As legal commentator Stewart Baker observed in 2012, "[a] kind of perfect storm has struck ZTE, ... [a] storm largely of ZTE's own making":

ZTE and its larger Chinese rival, Huawei, have been the subjects of great national security concern for years. The US intelligence community fears that, if allowed to install equipment here, the two companies will surreptitiously permit Chinese government wiretaps inside the United States. But proof of this suspicion has been hard to find. And the firms, backed by Chinese government-subsidized loans, have been able to offer enormous discounts to carriers, devastating the global telecom equipment market and leaving carriers eager to buy their products. Whether the US government would continue to act on its suspicions in the face of commercial pressure was an open question. ... Now, though, the mess is everywhere, and the House intelligence investigation will surely be heavily influenced by the new evidence that ZTE at least is quite capable of carrying out sophisticated telecommunications surveillance, of violating US law, and perhaps even lying about it later. Which, come to think of it, is pretty much what US intelligence agencies have been saying all along.²⁶⁷

.Indeed, ZTE is widely known to be an important geopolitical pawn for the Chinese Communist Party, with direct links to P.R.C. government and the People's Liberation Army through ZTE's substantial ties to the Chinese government and military apparatus.

799. China's Foreign Ministry confirmed its approval for ZTE's efforts to undermine U.S. national security when it expressed anger after the U.S. Commerce Department placed export restrictions on ZTE for violating U.S. export controls on Iran. "We hope the U.S. stops this erroneous action and avoids damaging Sino-U.S. trade cooperation and bilateral relations," Chinese Foreign Ministry spokesman Hong Lei said at a briefing in March 2012.

800. ZTE's aid for the IRGC and Qods Force are consistent with the Chinese Communist Party's desire to inflict pain on Americans in Afghanistan. The Chinese Communist Party views the United States being pinned down in conflict in the Middle East, and American

²⁶⁷ Stewart Baker, *And You Think You're Having A Bad Day?*, The Volokh Conspiracy (July 13, 2012), 2012 WLNR 14621514

being killed or injured in Iraq as beneficial to its interests. This is because protracted conflict in Iraq could give China the ability to expand its influence in the Middle East and could pin down the U.S. military in the Persian Gulf so that it is harder to pivot toward the Pacific.

801. That is why, from the Chinese Communist Party's perspective, there is strategic value in helping Iran develop enough military capabilities to counter U.S. dominance of the Persian Gulf. Indeed, Wang Jisi, Dean of the Peking University School of International Studies, has argued that the U.S. war with Iraq benefited China because "It is beneficial for our external environment to have the United States militarily and diplomatically deeply sunk in the Mideast to the extent that it can hardly extricate itself." Thus, a strong economic, diplomatic, and military partnership with the Islamic Republic could help China offset U.S. power in the Middle East. Similarly, Renmin University professor Shi Yinhong has recently argued that "Washington's deeper involvement in the Middle East is favorable to Beijing, reducing Washington's ability to place focused attention and pressure on China."

802. In 2021, Iran and China signed a deal expressing a desire to increase cooperation and trade relations over the next 25 years. It has been reported that this agreement enshrines a shared desire between China and Iran to reduce and resist U.S. influence in the region.

803. ZTE's agreement to aid Hezbollah, the Qods Force, and Regular IRGC served the Chinese Communist Party's agenda of inflicting pain on U.S. forces in Iraq. On information and belief, it also fulfilled an obligation by ZTE, similar to that of MTN, to engage in "defensive, security and political cooperation" with its IRGC, including Hezbollah and the Qods Force, partner.²⁶⁸ Such cooperation offered ZTE added motivation for ZTE's illicit transactions with Hezbollah, the Qods Force, and Regular IRGC. ZTE's support for Hezbollah, the Qods Force,

²⁶⁸ MTN Group-Irancell Consortium Letter Agreement § 8 (Sept. 18, 2005).

and Regular IRGC did not merely grow its profits by allowing it to obtain lucrative business from MTN Irancell and TCI in the first instance; it also benefited ZTE's business by inflicting harm on an enemy of ZTE's most important business partner (the Chinese Communist Party) and decisionmakers (the IRGC and Qods Force) in a key telecom market (Iran).

804. Plaintiffs' allegations also comport with the widespread view of relevant U.S. government officials from the executive and legislative branches. For starters, ZTE was forced to plead guilty and the largest criminal fine, to that date, in a United States sanctions case.

805. Moreover, a group of 33 Senators expressed concern about ZTE. In 2018, they sent a letter to President Trump indicating they viewed ZTE as a security threat. In relevant part the Democratic Senators (a) noted that ZTE violated US sanctions law and repeatedly lied about steps it would take to remedy the problems; (b) argued that America's national security must not be used as a bargaining chip in trade negotiations; (c) labeled ZTE as a "bad actor"; and (d) argued that loosening restrictions on ZTE could "risk American national security".

806. Concerns about ZTE's hostility to American national security are bipartisan. For example, Senator Marco Rubio has warned against allowing ZTE "to operate in U.S. without tighter restrictions," given national security and espionage concerns, and Senator Mark Warner has publicly reported to label ZTE as a "national security threat." Moreover, a multi-year bipartisan investigation by the House Select Committee on Intelligence concluded in October 2012 that ZTE "cannot be trusted to be free of foreign state influence and thus pose[s] a security threat to the United States and to our systems."

807. Further, the FCC recently designated ZTE as a "national security threat," and stated that "ZTE's violation of U.S. trade agreements and export laws, coupled with its obstruction of the Department of Justice's investigation, indicate a clear disregard for U.S. law

and national security.” Indeed, the FCC noted that ZTE has broken laws safeguarding U.S. national security, and ZTE has “shown a willingness to obstruct the investigations into such national security threats.” The FCC also observed “ZTE’s knowing violations of U.S. national security laws and its proven lack of cooperation in dealing with U.S. criminal investigators.”

808. OFAC, as well as the other U.S. government agencies, opened an investigation of ZTE in March 2012. As agreed by ZTE in its Settlement Agreement with OFAC, at or around that time, “an undisclosed person in ZTE’s legal department in Shenzhen called at least one ZTE employee present within the United States to instruct him to leave the country. These instructions were provided on the same day or shortly after search warrants were executed upon ZTE’s facilities located in the United States.” On information and belief, these statements relate to actions taken by employees of ZTE’s U.S. subsidiaries, including but not limited to ZTE USA.

809. As part of ZTE’s attempt to “cover up” its acts to provide U.S.-origin technology to TCI, ZTE and ZTE USA retaliated in the United States against the ZTE USA whistleblower in the United States who reported the scheme. ZTE also coordinated with ZTE USA in the United States and used ZTE USA as ZTE’s agent and instrumentality through which ZTE hired legal representation in the United States to respond to United States criminal investigations.

ii. ZTE’s Conduct Relied on American Contacts

810. ZTE reached into the United States to acquire U.S.-sourced embargoed technology that it then provided to Telecommunication Company of Iran and Aryacell.

811. TCI is predominantly state-controlled. TCI is owned by the Iranian regime and a private consortium with reported ties to IRGC, including Hezbollah and the Qods Force.

812. Aryacell is part of the consortium that, along with Hezbollah, the Qods Force, and Regular IRGC, controls TCI.

813. ZTE, including but not limited to in coordination with ZTE USA and ZTE TX, reached into the United States to support Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, when it obtained technology and vital operational support from the U.S. ZTE supplied technology and operational support for TCI and MTN Irancell through various U.S. agents, including but not limited to ZTE USA and ZTE TX. In doing so, ZTE tied its unlawful conduct to the United States by obtaining irreplaceable, best-in-class, and embargoed U.S.-supplied dual-use technology to aid the IRGC's, including Hezbollah's and the Qods Force's, terrorist enterprise. This U.S. contact was closely related to ZTE's, ZTE USA's, and ZTE TX's support for Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network.

814. ZTE relied on U.S.-made materials as components for its smartphones, cell phone systems, and computer networking gear. U.S.-origin goods were technically essential to ZTE's IRGC-related, including its Hezbollah Division-related and Qods Force-related, projects and/or end-users as there were no suitable foreign-made substitutes for many of them.

815. The embargoed United States technology included but was not limited to servers, switches, routers, and component parts of cellular network infrastructure.

816. The United States Commerce Department has said that ZTE sold prohibited American electronics to Iran to help Iran build its telecom networks.

817. Just about every product that ZTE makes has some American components or software in it, such as microchips, modems, and Google's Android operating system.

818. Public reports indicate ZTE helped funnel software and hardware from U.S. firms including Oracle, Microsoft, and Cisco Systems to the government of Iran in 2010 for use building what was described as a massive, nationwide surveillance system.

819. Simply put, ZTE could not do the business it did with Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, and thereby cause the transfer of key technology to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, without reaching into the United States to obtain that technology.

820. ZTE Corporation's regular transfers of communications technologies, including American cell phones, to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, relied upon American contacts, American transactions, American persons, and American service providers, and depended upon ZTE Corporation reaching into the United States, or causing agents, cut-outs, or affiliates to reach into the United States, in order to source the premium brand cell phones craved by al-Qaeda and the Taliban at all times after 9/11. On information and belief, from 2005 through present, ZTE Corporation regularly reached into the United States to acquire iconic American communication technologies for the Taliban's benefit, including, but not limited to, numerous technological generations, e.g., iPhone 5, iPhone 6, of: (i) Apple's iPhone and iPad, from California, which were among the most popular cell phones in the Middle East after 2008; (ii) Motorola's Two-Way Push-to-Talk Cell Phone, from Illinois, which was widely associated with Hezbollah and its proxies in the Middle East after the broad media coverage of their use during Hezbollah's 2006 attack campaign against Israel; and (iii) Motorola's Razr Cell Phone, from Illinois, which was one of the most popular cell phones in the Middle East before and after the iPhone.

H. The Huawei Defendants

1. Huawei Joined The Terrorist Conspiracy

i. Through Agreements With Hezbollah, Qods Force, And Regular IRGC Fronts, Including But Not Limited to TCI And Exit40, Huawei Agreed To Join A Company-Wide Conspiracy

821. Huawei and its subsidiaries—including Huawei USA, Huawei Device USA, Futurewei, and Skycom—joined the IRGC Conspiracy when they agreed to provide U.S.-origin goods and services, in violation of U.S. sanctions, to TCI and MTN Irancell, while knowing that TCI and MTN Irancell were fronts for Hezbollah the Qods Force, and Regular IRGC. Huawei and its subsidiaries—including Huawei USA, Huawei Device USA, Futurewei, and Skycom—agreement to join the Conspiracy was in the form of contracts that Huawei signed with TCI and, on information and belief, MTN Irancell and MCI. The IRGC Conspiracy was adopted by Huawei’s senior leadership and deployed throughout Huawei and its subsidiary Defendants.

822. On information and belief, Huawei and its subsidiaries, including Huawei USA, Huawei Device USA, Futurewei, and Skycom, furthered the IRGC Conspiracy when Huawei and its subsidiaries, including Huawei USA, Huawei Device USA, Futurewei, and Skycom, entered into an agreement to provide U.S.-origin goods and services, in violation of U.S. sanctions, to Exit40. This agreement in furtherance of the Conspiracy was in the form of contracts that Huawei signed with Exit40 and, on information and belief, MTN Irancell and MCI. This furtherance of the Conspiracy was adopted by Huawei’s senior leadership and deployed throughout Huawei and its subsidiaries, including Huawei USA, Huawei Device USA, Futurewei, and Skycom. Plaintiffs’ belief is based upon MTN Group’s retention of Exit40, which was for the same purpose and in response to the same IRGC instruction.

823. On information and belief, Huawei’s contracts with its IRGC-front Iranian counterparties all included pledges to assist with the “security” of Iran.

ii. Huawei Co., Huawei USA, Huawei Device USA, Futurewei, And Skycom Each Made Overt Acts In Furtherance Of The Conspiracy

824. Each of the Huawei Defendants, Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom, acted in furtherance of the Conspiracy by, *inter alia*: (a) sourcing

embargoed U.S.-origin technology useful to the terrorists for export to Hezbollah, the Qods Force, and Regular IRGC; (b) entering into contracts with U.S. suppliers to acquire the “\” technology essential to the terrorists; (c) stealing or otherwise misappropriating U.S.-origin technology and intellectual property from U.S. companies to deliver the same to Hezbollah, the Qods Force, and Regular IRGC; (d) developing and using third-party companies to both conceal and facilitate its business with IRGC-front companies; (e) commingling U.S.-origin technology with non-U.S.-origin technology in order to attempt to evade detection of the illicit transfers through the scheme that flowed aid to the IRGC; (f) providing U.S.-based financial services for its Iranian businesses; (g) lying to U.S. government authorities and financial institutions regarding the nature of their activities in Iran and their true IRGC-front counterparties; (h) destroying evidence related to the Conspiracy; (i) providing the services of a U.S. citizen for its Iranian subsidiary (Skycom) that concealed Huawei’s sourcing of U.S.-origin goods; and (g) moving one or more witnesses in the U.S. with knowledge of the scheme and Conspiracy outside of United States jurisdiction. Each act described above was in furtherance of the Conspiracy.

2. Huawei Knowingly Assumed A Financial, Logistical, And Operational Role In The IRGC’s, Including its Hezbollah Division’s And Qods Force’s, Terrorist Enterprise Against Americans Worldwide

825. Huawei bid on and secured contracts worth hundreds of millions of dollars to provide telecommunications and network infrastructure equipment and related services in Iran. Huawei knew that its counterparties were IRGC’s, including Hezbollah’s and the Qods Force’s, fronts, operatives, or agents. Huawei developed an elaborate system to fulfill those contracts using U.S.-origin items and services, which Huawei Co. did in collaboration with and with the assistance of Huawei USA, Huawei Device USA, Futurewei, and Skycom.

i. Huawei Co., Huawei USA, Huawei Device USA, Futurewei, And Skycom Knowingly Facilitated MTN Irancell And TCI Acquisition of Embargoed American Technology, Logistical

**Support, And Technical Services, Which Flowed Through To
The IRGC's Terrorist Proxies**

826. Huawei Co.'s, Huawei USA's (after its formation), Huawei Device USA's (after its formation), Futurewei's, and Skycom's company-wide scheme to obtain U.S.-origin goods and evade export controls to provide telecommunications technology to Hezbollah, the Qods Force, and Regular IRGC lasted from as early as 2008 and as late as 2014. To be clear, although Huawei USA was not formed until at least 2011 and Huawei Device USA was not formed until at least 2010, Plaintiffs allege that Huawei USA, Huawei Device USA, and their employees participated in the scheme to advance the Conspiracy after their respective formations.

827. The technology and equipment Huawei sourced from inside the United States was subject to the embargo imposed and enforced by the United States Government. Huawei thus violated export controls designed to keep sensitive American technology out of the hands of Hezbollah, the Qods Force, and Regular IRGC.

828. Through this scheme, which last at least between January 2008 and January 2014, Huawei exported U.S.-origin items to Hezbollah, the Qods Force, and Regular IRGC without obtaining proper export licenses.

829. The Huawei scheme operated in the Eastern District of New York, the Central District of California, the District of Columbia, the District of Delaware, the District of New Jersey, the Eastern District of Texas, the Northern District of California, the Northern District of Illinois, the Northern District of Texas, the Southern District of California, the Southern District of New York, the Western District of New York, the Western District of Washington and elsewhere, including overseas.

830. To circumvent the U.S. embargo and advance its Conspiracy with Hezbollah, the Qods Force, and Regular IRGC Huawei devised a scheme, whereby Huawei would set up

subsidiaries disguised as unrelated Iranian or Syrian “partners” and use those subsidiaries to hide Huawei’s business with, and shipment of prohibited U.S. technology to, the IRGC’s, including Hezbollah’s and the Qods Force’s, fronts, agents, and operatives. Skycom, which was controlled by Huawei, was one of Huawei’s subsidiaries to serve as an Iranian “partner” in this scheme.

831. After a series of international publications in 2012 publicly revealed Huawei’s sale of prohibited equipment to Iran, Huawei issued statements denying its involvement in violations of Iranian sanctions, as well as its ownership and control of Skycom. Despite the media revelations, Huawei continued sending U.S.-origin goods and services to the IRGC’s, including Hezbollah’s and the Qods Force’s, fronts, agents, and operatives.

832. In 2018, a federal grand jury indictment against Huawei Co., Huawei Device, Huawei Device USA, Futurewei, Skycom, and Wanzhou Meng (“Meng”) in *U.S. v. Huawei Technologies Co., Ltd., et al.* (E.D.N.Y. Case No. 1:18-cr-00457-AMD) (the “Huawei Criminal Case”) was unsealed, revealing numerous criminal charges against the Huawei Defendants relating to their scheme to support Huawei’s global business interests, including its efforts to provide embargoed goods and services to Iran. As detailed in the Superseding Indictment filed on February 13, 2020, in the Huawei Criminal Case, Huawei, including its American subsidiaries, including on information and belief Huawei USA, Huawei Device USA, and Futurewei, engaged in a series of unlawful conduct in and/or targeting the United States to carry out its scheme.²⁶⁹

833. As part of its international business model, Huawei engaged in business in countries subject to U.S., E.U. and/or U.N. sanctions, including Iran. This business, which

²⁶⁹ *United States v. Huawei Technologies Co., Ltd., et al.*, No. 18-457 (S-3) (AMD), 2020 WL 1319126 (E.D.N.Y. Feb. 13, 2020).

included shipping Huawei goods and services to end users in sanctioned countries, was typically conducted through local affiliates in the sanctioned countries, such as Skycom in Iran.

834. Even though the U.S. Department of the Treasury's ITSR, 31 C.F.R. Part 560, proscribed the export of U.S.-origin goods, technology and services to Iran and the Government of Iran, Huawei operated Skycom as an unofficial subsidiary to obtain otherwise prohibited U.S.-origin goods, technology and services, including banking services, for Huawei's Iran-based business while concealing the link to Huawei. Huawei could thus attempt to claim ignorance with respect to any illegal act committed by Skycom on behalf of Huawei, including violations of the ITSR and other applicable U.S. law, when providing U.S.-origin goods and services to Hezbollah, the Qods Force, and Regular IRGC.

835. At all relevant times, Skycom was owned and/or controlled by Huawei. In her Deferred Prosecution Agreement in the Huawei Criminal Case (dated September 22, 2021), Meng, Huawei Co.'s CFO and Deputy Chairwoman of its Board of Directors, and the daughter of its founder, admitted that between 2010 and 2014, (a) Huawei Co. controlled Skycom's business operations in Iran, (b) Skycom was owned by Huawei Co., (c) all significant Skycom business decisions were made by Huawei Co., (d) Skycom's country manager (for Iran) was a Huawei Co. employee, and (e) Huawei's prior denials of its control of Skycom were incorrect.

836. Meng was the Secretary of Hua Ying, a Huawei Co. subsidiary, when Huawei caused it to transfer its Skycom shares to Canicula, which was controlled by Huawei. After the transfer, Meng joined Skycom's Board of Directors, which was comprised of Huawei employees. Meng served on Skycom's Board until April 2009. After her departure, Skycom's Board members continued to be comprised of Huawei Co. employees. As of August 2012, Huawei included Skycom on a list of Huawei subsidiaries in Huawei Co. corporate documents.

837. Huawei's substantial efforts to circumvent U.S. sanctions and ensure a lucrative stake in the Iranian mobile network market is evidenced by its significant business with the largest (MCI) and second largest (MTN Irancell) Iranian mobile service providers, both of which are controlled by Hezbollah, the Qods Force, and Regular IRGC.

838. The success of MTN Irancell depended on its ability to source critical American technology and equipment for its systems and network, including, but not limited to, equipment from Sun Microsystems Inc., Oracle Corp., International Business Machines Corp., EMC Corp., Hewlett-Packard Co., and Cisco Systems, Inc., that were used to provide such services as wiretapping, voicemail, and text messaging.

839. Huawei, including its U.S. subsidiaries Huawei USA, Huawei Device USA, and Futurewei, leveraged its relationships and contracts with U.S. companies and research and development institutions to access and unlawfully export American equipment and technology through the Skycom scheme.

840. For example, in 2020, Huawei produced internal company records from 2010 evidencing its shipment of Hewlett-Packard equipment, including computer servers and switches, to MCI via Skycom, contrary to Huawei's prior denials about violating applicable sanctions and its ownership and control over Skycom.

841. At the time this transaction occurred, Huawei had a business relationship with Hewlett-Packard that allowed Huawei to incorporate Hewlett-Packard products into Huawei systems. Huawei took advantage of this arrangement to export surreptitiously embargoed U.S.-origin equipment and technology to Iran. Huawei's conduct was in violation of its distribution contract with Hewlett-Packard, which prohibited the sale of its products into Iran and required compliance with U.S. and other applicable export laws.

842. Huawei's internal company documents confirm that Huawei, including its U.S. subsidiaries Huawei USA, Huawei Device USA, and Futurewei, successfully procured and exported to Iran other U.S.-origin technology as well, including software made by Microsoft Corp, Symantec Corp, and Novell Inc. On information and belief, like it did with Hewlett-Packard, Huawei leveraged its relationships with these American companies to acquire and export U.S.-origin equipment and technology, in violation of its agreements with the American companies and U.S. law.

843. To further Huawei's global business interests, including its desire to export U.S.-origin equipment or technology to MCI and/or MTN Irancell, Huawei, including its U.S. subsidiaries Huawei USA, Huawei Device USA, and Futurewei, misappropriated and/or reverse-engineered US-origin equipment and technology.

844. As revealed by the Department of Justice's investigation, and subsequent indictment of Huawei Co., Huawei Device USA, and Futurewei for racketeering activity, Huawei and its subsidiaries engaged in a decades-long effort to misappropriate intellectual property, including from six U.S. technology companies, in an effort to grow and operate Huawei's business. The misappropriated intellectual property included trade secret information and copyrighted works, such as source code and user manuals for internet routers, antenna technology and robot testing technology.

845. Huawei, including Huawei USA, Huawei Device USA, Skycom, and Futurewei, and others executed a scheme to operate and grow the worldwide business of Huawei and its parents, global affiliates, and subsidiaries through the deliberate and repeated misappropriation of intellectual property of companies in the United States for commercial use.

846. The means and methods of the misappropriation included entering into confidentiality agreements with the owners of the intellectual property and then violating the terms of the agreements by misappropriating the intellectual property for Huawei's own commercial use, recruiting employees of other companies and directing them to misappropriate their former employers' intellectual property, and using proxies such as professors working at research institutions to obtain and provide the technology to Huawei and its subsidiaries.

847. As part of the scheme, Huawei launched a policy instituting a bonus program to reward employees who obtained confidential information from competitors. The policy made clear that Huawei employees, including employees of Huawei USA, Huawei Device USA, and Futurewei, who provided valuable information were to be financially rewarded by Huawei.

848. By misappropriating the intellectual property of the U.S. companies, Huawei received income directly and indirectly, including by benefitting from the sale of products containing stolen intellectual property to Hezbollah, the Qods Force, and Regular IRGC and saving on research and development costs, which income Huawei and its subsidiaries agreed to use to establish and operate the worldwide business of Huawei and its parents, global affiliates, and subsidiaries, including in the United States and Iran.

849. Huawei, including Huawei USA, Huawei Device USA, Skycom, and Futurewei, agreed to use the proceeds derived from the theft of U.S.-origin intellectual property to establish and operate the business of Huawei and its parents, global affiliates, and subsidiaries in the U.S. and abroad, including Iran.

850. Huawei, including Huawei USA, Huawei Device USA, Skycom, and Futurewei, agreed to benefit from the cost savings generated by stolen intellectual property to innovate more

quickly and to establish and operate the business of Huawei and its parents, global affiliates, and subsidiaries in the U.S. and abroad, including Iran.

851. Huawei USA's, Huawei Device USA's, and Futurewei's theft of American technology, trade secrets, and intellectual property under this scheme were directed by, and for the benefit of, Huawei Co. and Huawei's global business interests, including Huawei's agreements with Hezbollah, the Qods Force, and Regular IRGC. For example, as revealed in an investigation conducted by the Permanent Select Committee on Intelligence for the U.S. House of Representatives, several current and former employees of Huawei USA provided information indicating that Huawei USA is managed almost completely by Huawei Co. in China.

852. Huawei Co. controlled and directed each of its American subsidiaries' participation in its scheme to source U.S.-origin goods and services for Hezbollah, the Qods Force, and Regular IRGC and each of its American subsidiaries provided Huawei different channels by which Huawei could obtain or misappropriate U.S.-origin goods and services.

853. According to Huawei's public statements and disclosures, Huawei USA specializes in enterprise and network carrier business, Huawei Device USA focuses on the consumer business (e.g., handsets and routers), and Futurewei is Huawei's research and development arm. Thus, by directing each of its American subsidiaries to participate in its scheme to source U.S.-origin technology for Hezbollah, the Qods Force, and Regular IRGC Huawei created a comprehensive system for maximizing its procurement and export of U.S.-origin goods and services.

854. Huawei's scheme also included the provision of unlawful financial services to the IRGC's, including Hezbollah's and the Qods Force's, fronts, operatives, and agents.

855. In the Eastern District of New York and elsewhere, Huawei Co. and Skycom, together with others, conspired to cause the export, reexport, sale and supply, directly and indirectly, of banking and other financial services from the United States to Iran and the Government of Iran, without having first obtained the required OFAC license, contrary to Title 31, C.F.R., Sections 560.203, 560.204 and 560.206.

856. For example, after Huawei's Senior Vice President testified before U.S. Congress on September 13, 2012 that Huawei's business in Iran had not "violated any laws and regulations including sanction-related requirements" and other Huawei officers repeated those misrepresentations to financial institutions, Huawei Co. and Skycom completed the following unlawful financial transactions in America, involving U.S. banks, and/or international financial institutions and their U.S. subsidiaries: \$52,791.08 U.S.-dollar clearing transaction on July 24, 2013, \$94,829.82 U.S.-dollar clearing transaction on July 24, 2013, \$14,835.22 U.S.-dollar clearing transaction on August 20, 2013, \$32,663.10 U.S.-dollar clearing transaction on August 28, 2013, and \$118,842.45 U.S.-dollar clearing transaction on April 4, 2014.

857. Additionally, Huawei Co. and Skycom, together with others, knowingly and intentionally conspired to transport, transmit and transfer monetary instruments and funds, specifically wire transfers, from one or more places in the United States to and through one or more places outside the United States and to one or more places in the United States from and through one or more places outside the United States, with the intent to IEEPA. the

858. Huawei Co. repeatedly misrepresented to financial institutions that Huawei would not use the financial institution and its affiliates to process any transactions regarding Huawei's Iran-based business. However, Huawei used a U.S. subsidiary of a global financial institution and other financial institutions operating in the United States to process U.S.- dollar clearing

transactions involving millions of dollars in furtherance of Huawei's business with Hezbollah, the Qods Force, and Regular IRGC. Some of these transactions passed through this District.

859. As a result of Huawei's scheme and misrepresentations, financial institutions unwittingly cleared hundreds of millions of dollars in transactions that violated U.S. sanctions against doing business with Iran.

860. On information and belief, despite scrutiny from the media, financial institutions, and governmental authorities, Huawei never ceased sourcing U.S.-origin goods and services to Hezbollah, the Qods Force, and Regular IRGC. In addition to sourcing the requested U.S.-origin products and services in contravention of U.S. law, Huawei aggressively pursued relationships with IRGC's, including Hezbollah's and the Qods Force's, fronts, agents, and operatives to protect its lucrative business interests in Iran.

861. While many international vendors withdrew from the Iranian market to avoid violating sanctions, Huawei aggressively secured numerous contracts with both MTN Irancell and MCI to provide telecommunications equipment and services. As reported by the *Wall Street Journal* on October 27, 2011, Huawei secured numerous contracts with both MCI and MTN Irancell, and in doing so, agreed to carry out orders from, and support the interests of, Hezbollah, the Qods Force, and Regular IRGC.²⁷⁰

862. The *Wall Street Journal* reported, in relevant part, that Huawei "filled the vacuum" after "Western companies pulled back from Iran after the government's bloody crackdown on its citizens," and thereby, Huawei "plays a role in enabling Iran's state security network." *Id.* The *Wall Street Journal* further reported that "a person familiar with Huawei's

²⁷⁰ Steve Stecklow, Farnaz Fassihi, and Loretta Chao, *Chinese Tech Giant Aids Iran*, Wall St. J. (Oct. 27, 2011).

Mideast operations” said Huawei’s role included “overseeing parts of the network -- at MTN Irancell, which is majority owned by the government,” and that in 2009 Huawei “carried out government orders on behalf of its client, MTN Irancell, that MTN and other carriers had received to suspend text messaging and block the Internet phone service, Skype, which is popular among dissidents.” *Id.*

863. Huawei’s agreement to abide by the directives of Hezbollah, the Qods Force, and Regular IRGC was openly promoted by Huawei and the Chinese government. For example, in August 2009, two months after the mass protests began in Iran, the “website of China’s embassy in Tehran reprinted a local article under the headline, ‘Huawei Plans Takeover of Iran’s Telecom Market.’ The article said the company ‘has gained the trust and alliance of major governmental and private entities within a short period,’ and that its clients included ‘military industries.’” *Id.*

864. Huawei’s agreement to abide by the directives of the IRGC’s, including Hezbollah’s and the Qods Force’s, fronts, operatives, or agents, was not limited to its work with MTN Irancell. Huawei secured contracts with the largest Iranian mobile network provider MCI, which is controlled by TCI, by expressly agreeing to provide support for the IRGC’s, including Hezbollah’s and the Qods Force’s, “security” and intelligence objectives. Huawei also has direct contractual ties to TCI.

865. In fact, to secure its place in the Iranian market, Huawei has done “considerable business” with Zaeim Electronic Industries Co. (“ZEI”), an Iranian electronics firm, which is the “**security** and intelligence wing of every telecom bid.” ZEI launched its telecommunications division in 2000 in partnership with Huawei and have completed at least forty-six telecommunication projects together. ZEI’s website noted its clients include “the intelligence

and defense ministries, as well as the country's elite special-forces unit, *the Islamic Revolutionary Guards Corps*.” *Id.* (emphasis added).

866. On information and belief, ZEI was a front for Hezbollah, the Qods Force, and Regular IRGC. ZEI was responsible for “security” functions on more than one IRGC-facing project with respect to more than one Western customer, ZEI was closely linked to multiple IRGC addresses and persons, and independent observers concluded the IRGC ran it. *Id.*

867. Huawei also assisted the IRGC’s, including Hezbollah’s and the Qods Force’s, fronts, agents, and operatives by installing surveillance equipment, including surveillance equipment used to monitor, identify, and detain protestors during the anti-government demonstrations of 2009 in Tehran, Iran.

868. As reported by the *Wall Street Journal*, and similar to MTN’s agreement to assist with “security,” Huawei agreed as part of its bid to install MCI’s surveillance system to “support and deliver offline and real-time lawful interception,” and that, “for public security,” the service would allow “tracking a specified phone/subscriber on map.”

869. Huawei’s scheme to provide assistance to the IRGC’s, including Hezbollah’s and the Qods Force’s, fronts, operatives, and agents was not limited to the sourcing of U.S.-origin equipment and technology. For example, Skycom, on behalf of Huawei, employed a U.S. citizen in Iran. Huawei and Skycom were indicted for this unlawful provision of U.S.-based services.

870. Huawei modernized telecommunications technology used by Iranian entities that were controlled by IRGC, including Hezbollah and the Qods Force, fronts, thereby pumping additional revenue into the coffers of Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network.

871. Huawei Co., Huawei USA (after its formation), Huawei Device USA (after its formation), Futurewei, and Skycom provided substantial banned technology to Iranian companies that were controlled by Hezbollah, the Qods Force, and Regular IRGC and, thereby, Huawei's illegally sourced technology ordinarily flowed through to Hezbollah. That banned technology was crucial to enabling terror. For example, terrorists were able to use cell phones and other telecommunication technology and software to perpetrate attacks on Americans.

872. Huawei also assisted the terrorist enterprise by serving as a long-term strategic partner for MTN Irancell and MCI, both of which were fronts for Hezbollah, the Qods Force, and Regular IRGC.

873. Like ZTE, on top of the millions of dollars that Huawei provided to Hezbollah, the Qods Force, and Regular IRGC via TCI (and MCI), Huawei also provided technical aid, including surveillance technology, to Hezbollah, the Qods Force, and Regular IRGC which facilitated terrorism. Huawei Co.'s, Huawei USA's (after its formation), Huawei Device USA's (after its formation), Futurewei's, and Skycom's technology transfer provided terrorists the ability to intimidate and coerce civilian populations.

874. For a terrorist group intent on targeting Americans traveling in tightly secured convoys or on heavily fortified bases, the technology that Huawei provided bolstered the terrorists' ability to conduct successful surveillance and was vitally important to their ability to execute successful attacks, like the ones that killed and injured Plaintiffs and their loved ones. For these reasons, Huawei's acts, which allowed terrorists access to modern telecommunications technology they could not otherwise obtain, facilitated intimidation, coercion, violent acts, and acts dangerous to human life.

875. The ample evidence of Huawei's own consciousness of guilt supports the inference that Huawei knew it was benefiting the IRGC's, including Hezbollah's and the Qods Force's, terrorist enterprise.

876. As part of the scheme to operate and advance the business of Huawei, including its agreement with the IRGC, Huawei, Huawei Device USA, and Futurewei sought to avoid interference in their scheme by U.S. governmental bodies or other private actors by repeatedly making material misrepresentations as to their misappropriation and subsequent commercial use of intellectual property, as well as other criminal activity, including the nature and extent of Huawei's business in Iran, to U.S. governmental bodies from whom Huawei, Huawei Device USA, and Futurewei sought regulatory authorization that would help grow Huawei's U.S.-based business.

877. Huawei, Huawei Device USA, and Futurewei made similar material misrepresentations to financial institutions from whom the Defendants sought banking services to process Huawei's and Skycom's Iranian business transactions.

878. Huawei, Huawei USA, Huawei Device USA, and Futurewei made material misrepresentations to the U.S. government about the nature and the scope of Huawei's business activities related to sanctioned countries such as Iran and North Korea, to avoid the economic and regulatory consequences of making truthful statements, including the restriction of Huawei from U.S. markets and business opportunities.

879. In or about 2017, Huawei Co. and Huawei Device USA became aware of the U.S. government's criminal investigation of Huawei and its affiliates. In response to the investigation, Huawei and Huawei Device USA made efforts to move witnesses with knowledge about Huawei's Iran-based business out of the United States and to the People's Republic of

China, so that they would be beyond the jurisdiction of the U.S. government, and to destroy and/or conceal evidence located in the United States of Huawei's Iran-based business.

ii. Huawei Substantially Increased MTN Irancell And TCI Revenue By Illicitly Sourcing Embargoed U.S. Technology, Which Flowed Through To The IRGC's Terrorist Proxies

880. From 2008 through at least 2014, Huawei Co.'s, Huawei USA's, Huawei Device USA's, Futurewei's, and Skycom's illicit transactions with MTN Irancell, the Bonyad Mostazafan, IEI, TCI (including MCI), Exit40, and/or the Akbari Fronts, provided millions, annually, in illicit funds, weapons, and operational support to Hezbollah, the Qods Force, and Regular IRGC which flowed to al-Qaeda and the Taliban and was used to attack Americans in Afghanistan, including Plaintiffs and their loved ones.

881. Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom significantly increased the cash flowing through MTN Irancell and TCI, and ultimately being deployed by Hezbollah, the Qods Force, and Regular IRGC. They did so by illicitly supplying the state-of-the-art American technologies, like servers, to MTN Irancell and TCI, and by extension Hezbollah, the Qods Force, and Regular IRGC needed to attack Americans abroad.

iii. Huawei Routed Bribes To The Key Procurement Decisionmakers At MTN Irancell And TCI, Which Flowed Through To The IRGC's Terrorist Proxies

882. Huawei Co. has an extensively documented record of paying bribes around the world in order to win lucrative procurement contracts. Huawei has been credibly accused of procurement-related corruption in, *inter alia*, Namibia.

883. Huawei Co. has pursued an integrated global sales strategy, under which one may infer that Huawei Co. followed the same, or a substantially similar, bribery tradecraft with respect to similar "pitches" for other state-owned telecom companies.

884. According to the Organized Crime and Corruption Reporting Project (“OCCRP”), Huawei Co.’s “going rate” for bribing decision-makers in the procurement contract setting appears to be at least approximately one percent (1%) of contract value.

Huawei appears to have paid large sums to a former Serbian state telecom executive through an offshore shell company.

The Chinese tech giant Huawei signed deals to make large payments to two men close to Serbia’s state telecommunications company, using offshore companies that financial crime experts say raise red flags for corruption.

One of these men, former Telekom Srbija executive Igor Jecl, appears to have received over \$1.4 million in contracts, dividends, loans, consulting fees, and an apartment from an offshore company that was paid by Huawei for consultancy. Neither offshore company that dealt with Huawei has a public track record of doing consulting work, or any business at all.

“It is standard with bribery and corruption to dress them up as consultancy,” said Graham Barrow, an expert on financial crime.

Although OCCRP has not uncovered evidence that the payments were improper, they were made over a period of time when Huawei was doing business in Serbia. In 2016, it landed a 150-million-euro deal to upgrade Serbia’s telecommunications infrastructure.²⁷¹

885. On information and belief, from 2008 through 2018, Huawei Co. caused the payment of at least several million dollars, denominated in U.S. Dollars, to one or more officers, agents, or directors of MTN Irancell, TCI, and/or MCI.

iv. The Huawei Defendants Routed “Free Goods” To The Key Procurement Decisionmakers At MTN Irancell And TCI, Which Flowed Through To The IRGC’s Terrorist Proxies

886. Huawei Co. has a documented history of making a species of “free goods” payment – giving something away at below market pricing to obtain a collateral benefit.

²⁷¹ Stevan Dojčinović and Vesna Radojević, *The Pandora Papers: Chinese Tech Giant Huawei Had Secret Offshore Contracts With Men Linked to Serbian State Telecom Company*, Organized Crime and Corruption Reporting Project (Oct. 25, 2021), <https://tinyurl.com/26n3rayt>.

887. On information and belief, Huawei Co. has pursued a similar “free goods” bribery strategy through the sale of below-market-priced technologies to its IRGC-affiliated customers.

3. Huawei Knowingly Assumed A Financial, Logistical, And Operational Role In The Taliban’s, Including The Haqqani Network’s, Terrorist Enterprise In Afghanistan, Directly And Indirectly Financing And Arming IRGC Proxy Attacks In Afghanistan And Iraq

888. Huawei operated lucrative businesses in post-invasion Afghanistan by servicing a broad array of customers there. To increase their profit margins by redirecting attacks away from their business interests – and to intentionally assist the Taliban’s effort to drive Americans out of Afghanistan – Huawei knowingly paid protection money to the Taliban, including its Haqqani Network. When Huawei did so, Huawei knowingly assumed a financial, logistical, and operational role in the Taliban’s, including the Haqqani Network’s, terrorist enterprise in Afghanistan and beyond by directly and indirectly routing protection payments to these terrorists in cash and “free goods,” including secure American cell phones.

889. Huawei has become one of the world’s most valuable communications technology manufacturers by providing a comprehensive suite of communications technologies services to customers in high-risk geographies from a counter-terrorism perspective, including geographies where Hezbollah, the Qods Force, and Regular IRGC and IRGC proxies al-Qaeda and the Taliban, including its Haqqani Network, raised and moved money to facilitate terrorist attacks through protection payments, procurement corruption, “free goods” payoffs, payments routed through consultants, and similar schemes that depended upon complicit corporate partners.

890. Huawei followed that model in Afghanistan, where Huawei has continuously operated for decades.

891. For example, in 2001, “India's intelligence agencies” “placed” “the Chinese telecommunications equipment maker Huawei Technologies Inc.[’s] Indian operations on a

watch list for alleged business dealings with the Taliban” after “Indian government” concluded “that Huawei India allegedly helped supply communications surveillance equipment to Taliban forces in Afghanistan.”²⁷²

892. Huawei’s willingness to directly partner with the Taliban, continued even after al-Qaeda and the Taliban had launched their nationwide campaign against Americans in Afghanistan after 9/11. Indeed, Huawei was a preferred partner of the Haqqani Network in Pakistan and Afghanistan because Huawei regularly paid the amount requested by the Taliban. In 2005, for example, the Economic Times (of India) reported how “[a] western multinational telecom company executive was being badgered by a senior bureaucrat to set up a full-fledged mobile network in Jammu and Kashmir,” which were two Pakistani hotbeds for the Syndicate:

Given the security environment ..., and kamikaze not exactly being the guiding philosophy of his [western multinational telecom] company, he had to decline the offer but managed to come up with what he thought was a viable alternative. Since a working relationship with the militants and the Taliban is an essential prerequisite for sustaining operations in the state, why don't you ask Huawei to take on the task? Well, why not? After all, the [Indian] government has been claiming that Huawei Technologies, the Chinese telecom major, has had links with the Taliban when they ran Afghanistan.²⁷³

893. From 2006 through 2019, Huawei sold products to Afghan telecommunications operators, e.g., MTN Afghanistan, which was MTN’s subsidiary in Afghanistan, which were manufactured by the Huawei Defendants.

894. While Huawei was achieving rapid growth in Afghanistan, the communications sector provided a critical source of financing for the Taliban, including its Haqqani Network, in the same manner as it did for Defendants ZTE and MTN. Huawei’s payments mirrored the

²⁷² K.C. Krishnadas, *India: Chinese Telecom Firm Supplied Taliban*, Electronic Engineering Times (December 17, 2001), 2001 WLNR 3069135.

²⁷³ Economic Times (India), *Satyajit Ray Who?* (Sept. 20, 2005), 2005 WLNR 29155896.

protection money delivered by ZTE and MTN. Just as the Taliban raised “taxes” from international contractors doing business in Afghanistan, so too did it levy similar “taxes” on “the big telecom companies” like Huawei.²⁷⁴

895. Huawei’s services in Afghanistan required Huawei work in geographies that were controlled or contested by the Taliban, including its Haqqani Network, in which Huawei paid protection payments as a cost of doing business.

896. Huawei’s sales to its Afghan customers depended upon Huawei personnel successfully driving large truck convoys containing Huawei’s lucrative Afghan-customer-bound goods through Taliban, including Haqqani Network, controlled or contested geographies in Pakistan and Afghanistan.

897. Huawei paid the money as protection: Huawei decided that the cheapest way to shield their projects from attack was to pay the Taliban, including its Haqqani Network to leave them alone and instead attack other targets – like Plaintiffs and their family members. Similar payments were pervasive throughout Afghanistan and supplied the Taliban with an important stream of financing to fund their terrorist attacks across the country.

898. The Taliban, including its Haqqani Network, conveyed its protection-money demands to Huawei via Night Letters similar the ones the Taliban sent to ZTE and MTN.

899. Huawei was a particularly aggressive practitioner of protection payments. Rather than invest in expensive security for shipments, Huawei purchased cheaper “security” by buying it from the Taliban, including its post-FTO-designation Haqqani Network.

900. Huawei negotiated its protection payments in direct discussions between Huawei Afghanistan’s security department and Taliban, including Haqqani Network, commanders.

²⁷⁴ Ruttig, *The Other Side* at 20.

901. Like other contractors in Afghanistan, Huawei generally paid, as protection to the Taliban (including its Haqqani Network), at least ten percent (10%) of its contract budget – and, on information and belief, much more than this – on any contract in which Huawei, including any Huawei affiliate or contractor, provided services to any customer in Afghanistan, since the Taliban controlled or contested every geography in which Huawei worked.

902. Huawei’s practice of making protection payments to the Taliban extended to the Haqqani Network. From at least 2008 through 2017, Huawei operated infrastructure projects sites, and/or sold communications technology products to customers (and therefore transported lucrative commodities through territory) in Afghanistan that was controlled by the Haqqani Network, and Huawei purchased security for those project sites and shipments by paying the Haqqani Network. The Haqqani Network’s chief financial operative, Nasiruddin Haqqani, oversaw those payments, and they typically occurred on a semi-annual basis, and the Haqqani Network’s overall involvement in the scheme was ultimately supervised by Sirajuddin Haqqani, who was at all times a dual-hatted al-Qaeda/Taliban terrorist.

903. Huawei keyed Huawei’s rapid growth in Afghanistan by sponsoring a vast stream of payoffs to the Haqqani Network from 2006 through today. Under Sirajuddin Haqqani’s leadership, as executed by his immediate family members, the Haqqani Network was responsible for collecting “taxes” from Afghanistan’s telecom companies, which were the single largest (legal) industry and tax base in Afghanistan – and thus a key source of funding and power for the Taliban and al-Qaeda, both of which were effectively led by Sirajuddin Haqqani.

904. The logic behind Huawei’s payoffs to the Haqqani Network matched the logic motivating Huawei’s joint venture with the IRGC. Huawei’s leadership intended to harm American interests in Afghanistan (like Iraq), and supporting the Taliban allowed them to do so.

Huawei's decision to route monthly protection payments to al-Qaeda (via Sirajuddin Haqqani and his immediate family members) and the Taliban was made so that Huawei would not face the risk that terrorists commanded by Sirajuddin Haqqani would destroy some of Huawei's shipments. Ordinarily, the going protection payment rate was usually around \$500 to \$2,000 per truck per convoy. In some areas, Huawei caused payments to be made to local Taliban, including Haqqani Network, commanders. In other places, where Huawei operated in a Taliban-controlled environment, the payments would have to be sent to the Taliban's Quetta Shura for southern Afghanistan, e.g., Helmand, or the Taliban's Miram Shah Shura for eastern Afghanistan, e.g., Paktia (Sirajuddin was involved in the former and led the latter).

905. By 2006, the Taliban, including its Haqqani Network, prized the acquisition of Western communications technologies, including American-made cell phones, that were "washed" through the IRGC or one of its corporate partners, like Huawei.

906. From 2006 through 2021, Huawei also made protection payments to the Taliban, including its Haqqani Network, in the form of "free goods" – in particular, free communications technologies like cell phones – as an alternative to paying the terrorists in cash. When Huawei did so, Huawei directly provided to the Taliban, including its Haqqani Network, a broad range of communications technologies including, but not limited to, American mobile phones such as American-made Motorola phones, which Huawei reached into the U.S. to specifically acquire for the purpose of transferring such technologies to the IRGC and its proxies, including the Taliban.

907. On information and belief, Huawei transferred millions of U.S. Dollars' worth of American communications technologies, including more than a thousand (1,000) "free goods" black market American-made cell phones to the Taliban, including its Haqqani Network, which

Huawei acquired from the United States and delivered to the Taliban, including its Haqqani Network, each year from 2006 through 2021.

908. Huawei’s transfer of free, and illicitly sourced, communications technologies, including technologies that Huawei sourced from the United States, as a means to bribe the Taliban, including its Haqqani Network, comports with Huawei’s long-standing embrace of “free goods” as a core, decades-long, global strategy to route bribes to recipients.

909. U.S. military and intelligence officials have publicly confirmed Plaintiffs’ allegations against Huawei. For example, on June 8, 2012, *Business Insider* confirmed – citing American “military sources” and “former and current intelligence sources” – that that “China [was] likely to remain an aggressive and capable collector of sensitive U.S. economic information and technologies.”²⁷⁵ Thus, “[a]nother concern raised by [U.S. military] sources [was] that Huawei and the other Chinese telecommunications companies [i.e., ZTE] also provide[d] technology to Iran and the Taliban.” *Id.* Indeed, “[a]ccording to sources, Iran’s security network relie[d] on Huawei technology.” *Id.*

910. When Huawei provided free communications technologies to the Taliban, including black market American cell phones, Huawei provided the terrorists a cash equivalent that sponsored tremendous violence. At a going rate of \$2,000 per black market cell phone, for example, the value of Huawei’s illicit phones supplied to the Taliban, including its Haqqani Network, delivered at least \$2 million per year in value to the Taliban.

911. When Huawei acquired and transferred free communications technologies to the Taliban, including black market American cell phones, from the United States and delivered such technologies to the Taliban, including its Haqqani Network, Huawei provided devastating

²⁷⁵ *Business Insider*, *supra* note 142.

operational and logistical assistance to the Syndicate in addition to the financial value of such goods through the same operational and logistical benefits that such black market communications technologies, including American cell phones, accorded to terrorists worldwide.

912. Huawei also directly aided al-Qaeda when Huawei transferred cash and free goods, including the above-described communications technologies and black market American cell phones, to the Haqqani Network because Sirajuddin Haqqani and his immediate family members, who were responsible for collecting protection payments from telecom companies like Huawei, were also members of al-Qaeda, and thus Huawei funded and logistically supplied al-Qaeda when Huawei routed cash and free goods protection payments to the Haqqani family.

913. Huawei's overall payments to the Taliban, including its Haqqani Network, reached millions of dollars in value in cash and "free goods" payments of communications technologies, including black market American cell phones each year from 2006 through the present. At that rate, the Huawei Defendants caused at least tens of millions in U.S. Dollar-value in cash and "free goods" to flow through to the Taliban, including its Haqqani Network, from 2006 through the present, which furthered the IRGC Conspiracy to attack Americans in Afghanistan and directly aided the IRGC proxies who committed such attacks, i.e., al-Qaeda and the Taliban through attacks committed by joint al-Qaeda/Taliban cells and/or attacks committed by the Taliban that were planned and authorized by al-Qaeda.

4. Huawei's Assistance To Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, And The Taliban, Comports With Huawei's Historical Business Practices In International Markets

914. Like MTN and ZTE, Huawei's conduct reflected a willingness to support America's enemies and engage in illicit financial transactions as a way to increase profits in Iran. The same calculation pervaded Huawei's other conduct throughout the world. Huawei's other

conduct further demonstrates its pattern and practice of transacting with violent actors to increase Huawei revenue.

915. Huawei's illicit transactions concerning North Korea demonstrates Huawei's deliberate support for terror.

916. On or about September 13, 2012, a Huawei representative testified before U.S. Congress, testifying that Huawei was not involved in North Korean business interests after 2009. As the Superseding Indictment notes, however, "Huawei was involved in business activities in North Korea, including numerous telecommunications projects, beginning no later than 2008."

917. Internal Huawei documents obtained by the Department of Justice referred to the geographic location of projects in North Korea with the code "A9"—Huawei's code for North Korea. Huawei employees concealed Huawei's involvement in projects in North Korea.

918. For example, shipping instructions provided by Huawei to a supplier in 2013 included the instruction that, for shipments to "A9/NK/NORTH KOREA," there should be "No HW [HUAWEI] logo," indicating that Huawei's corporate logo should not be included on shipments destined for North Korea.

919. Plaintiffs' allegations concerning Huawei's willingness to pay bribes and protection payments, in cash and free goods, are also consistent with Huawei's recent history, as documented by press reports concerning allegations of "rampant corruption" and programmatic bribery by Huawei around the world for decades.²⁷⁶

²⁷⁶ See, e.g., Technode.com, *Another Corruption Scandal Hits Huawei With Its Top Executive Suspected Of Bribery* (Dec. 26, 2017) ("The executive vice president of Huawei's consumer business group Greater China, Teng Hongfei, has been taken away by the public security... Once a recipient of the highest management honor granted by Huawei, Teng is under investigation for corruption charges... Teng's fall from grace might have been a result of the rampant corruption inside China's direct-to-consumer sales, in which retailers often bribe the manufacturers... This

5. Huawei's Assistance To Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, And The Taliban Had A Substantial Nexus To The United States

920. Huawei's assistance to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, relied on significant contacts with the United States. Huawei orchestrated both those U.S. contacts and Huawei's violation of U.S. law, including, on information and belief, by and through coordination with Skycom, Huawei Device USA, Huawei USA, and Futurewei. Like MTN and ZTE, Huawei employed a top-down management structure in which Huawei centralized operational control over the functions performed by its subsidiaries.

921. Huawei's decision to assist Hezbollah, the Qods Force, and Regular IRGC and by extension their proxies, al-Qaeda and the Taliban, had a substantial nexus to the United States for the reasons explained below.

i. Huawei's Conduct Targeted the United States

922. Huawei's provision of material support to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, was expressly aimed at the United States. At all relevant times, Huawei knew that Hezbollah, the Qods Force, Regular

isn't the first time Huawei has found itself in the midst of a corruption scandal. This year started with a bang when six top middle and senior leaders from the consumer business group were accused of giving out internal information...One of the arrested employees was the chief architect of Huawei's flagship P6 Wu Bin... In 2012, Huawei also found itself in trouble in international waters when Huawei's Xiao Chunfa was sentenced by an Algerian court along with two other staffers from Chinese smartphone maker ZTE. The trio was tried in absentia for a bribery scandal... They were sentenced to ten years in prison..."), *online at* <https://tinyurl.com/2a9nnsas> (last accessed Apr. 3, 2022); Wall St. J., *Huawei Internal Probe Finds Possible Evidence of Corruption; Internal Probe Finds 116 Employees May Have Been Involved in Corruption* (Sept. 11, 2014) ("Huawei Technologies Co. said [] that a recent internal investigation has found that 116 of its employees may have been involved in corruption... The Chinese telecommunications equipment maker ... didn't provide any further details about the employees in question or the bribery allegations... Chinese media reported last month that Huawei found possible evidence of corruption cases involving 116 employees and hundreds of millions of yuan in bribery.").

IRGC, al-Qaeda, and the Taliban, were targeting the United States. Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, did not conduct an indiscriminate terrorist campaign that merely injured Americans by chance. Instead, Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, directed attacks at *Americans* with the specific intent of killing *Americans* in particular – so that they could inflict pain in the United States and influence U.S. policy. Hezbollah’s, the Qods Force’s, Regular IRGC’s, al-Qaeda’s, and the Taliban’s, including its Haqqani Network’s, ultimate, shared, publicly stated goal was to effect a withdrawal of American forces from Afghanistan and the broader Middle East. Each terrorist attack that killed and injured Plaintiffs was part of that campaign of anti-American terrorism.

923. Huawei’s decision to reach into the United States, including by coordinating with Huawei USA, Huawei Device USA, and Futurewei, to obtain embargoed technology to aid the IRGC’s, including Hezbollah’s and the Qods Force’s, terrorist enterprise was also expressly aimed at the United States. Like MTN and ZTE, Huawei knew, based on conversations with IRGC, including Hezbollah and the Qods Force, agents, that Hezbollah, the Qods Force, and Regular IRGC viewed Huawei’s assistance as vital to Iranian national “security,” which Huawei understood to inherently involve the promotion of terrorist violence against Americans around the world as part of Hezbollah’s, the Qods Force’s, and Regular IRGC’s effort to export its Islamic Revolution and drive the U.S. out of Afghanistan.

924. On information and belief, like MTN and ZTE, Huawei also knew, based on conversations with U.S. officials, that it was assuming an active role in a Hezbollah, Qods Force, and Regular IRGC plot to develop cash flow and source vital dual-use components for their terrorist proxies, including al-Qaeda and the Taliban. Huawei further knew of the critical importance that communications and computing technology plays for terrorists.

925. When Huawei Co., including by coordinating with Skycom, Huawei USA, Huawei Device USA, and Futurewei, conducted U.S.-based financial transactions denominated in U.S. dollars and sourced embargoed technology that the United States had publicly declared could benefit IRGC, including Hezbollah and the Qods Force, efforts to kill Americans, they intentionally helped arm terrorists they knew were targeting the United States. On information and belief, Hezbollah, the Qods Force, and Regular IRGC made Huawei agree to a similar contractual pledge as the one in which MTN agreed to aid Iran's "defensive, security, and political" interests outside of Iran. On information and belief, at all times, Huawei knew or recklessly disregarded that "security" was a euphemism for IRGC, including Hezbollah and the Qods Force, terrorist operations outside of the territorial borders of Iran. When Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom executed financial transactions and obtained the technology requested by its IRGC, including Hezbollah and the Qods Force, partners, each took actions in the United States and targeted at United States by helping the terrorists improve their bombs, rockets, communications, and intelligence gathering.

926. Although Huawei's primary motivation for assisting Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban was financial, Huawei also intended to harm Americans in Afghanistan. One reason Huawei cooperated with Hezbollah, the Qods Force, and Regular IRGC was to align itself with their effort to drive Americans out of Afghanistan.

927. Like MTN and ZTE, Huawei intended to harm Americans because it decided that was the necessary price of maintaining a good relationship with Hezbollah, the Qods Force, and Regular IRGC who were explicit, that they expected their partners to provide significant help in fighting against U.S. forces in particular. Thus, for Huawei to achieve its business objectives vis-à-vis Hezbollah, the Qods Force, and Regular IRGC fronts who controlled TCI (including

MCI) and MTN Irancell – both of which Huawei serviced – Huawei needed to disassociate itself from the United States and prove that it could deliver value to the IRGC’s terrorist campaign against U.S. forces in Afghanistan.

928. On information and belief, like MTN, Huawei’s agreement to aid Hezbollah, the Qods Force, and Regular IRGC also fulfilled an obligation by Huawei, like MTN, to engage in “defensive, security and political cooperation” with its IRGC, including Hezbollah and Qods Force, counterparties.²⁷⁷ Such cooperation offered Huawei added motivation for Huawei’s illicit transactions with Hezbollah, the Qods Force, and Regular IRGC counterparties. Huawei’s support for Hezbollah, the Qods Force, and Regular IRGC did not merely grow Huawei’s profits by allowing it to obtain lucrative business from MTN Irancell and TCI (and MCI) in the first instance; it also benefited Huawei’s business by inflicting harm on an enemy (the United States) of one of Huawei’s most important business partners (Hezbollah, the Qods Force, and Regular IRGC) in order for Huawei to curry Iranian favor to gain market share for a potentially uniquely lucrative telecom and communications market (Iran).

929. Plaintiffs’ allegations also comport with the widespread view of relevant U.S. government officials from the executive and legislative branches. For starters, Huawei and its subsidiaries are subject to multiple criminal proceedings for their unlawful conduct with respect to Iran, including the Huawei Criminal Case.

930. Huawei’s scheme to source U.S.-origin technology for Hezbollah, the Qods Force, and Regular IRGC also serves and/or conforms to the People’s Republic of China’s broader security and economic interests of competing against the U.S.

²⁷⁷ Exhibit A, MTN Group-Irancell Consortium Letter Agreement § 8.

931. For example, the Chinese government arrested and jailed several Huawei whistleblowers who claimed that Huawei's business in Iran is an "open secret" and made some of these whistleblowers sign statements pledging to not go against Huawei's public position denying the nature and scope of its Iranian business.

932. Moreover, Huawei previously worked with Panda International Information Technology Co., Ltd. ("Panda Int'l"), a Chinese-state-owned firm, in their joint efforts to help build and maintain North Korea's wireless network using embargoed goods, and to conceal Huawei's sanctions-busting conduct. Huawei also partnered with Panda in Iran. Thus, Huawei's prior conduct reflects its deference to, and support for, the broader security and economic objectives of the People's Republic of China.

ii. Huawei's Conduct Relied on American Contacts

933. Huawei reached into the United States to acquire U.S.-sourced embargoed technology that it then provided to MTN Irancell, MCI, and, on information and belief, TCI.

934. Huawei Co., including but not limited to in coordination with Huawei Device USA, Huawei USA, Futurewei, and Skycom, reached into the United States to support Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, when it obtained technology and vital operational support from the U.S. Huawei supplied technology and operational support for TCI, MCI, and MTN Irancell through various U.S. agents, including but not limited to Huawei Device USA, Huawei USA, and Futurewei. In doing so, Huawei tied its unlawful conduct to the United States by obtaining irreplaceable, best-in-class, and embargoed U.S.-supplied dual-use technology to aid Hezbollah's, the Qods Force's, and Regular IRGC's terrorist enterprise. This U.S. contact was closely related to Huawei's support for Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban.

935. Huawei relied on U.S.-made materials as components for its products for Iran. U.S.-origin goods were technically essential to Huawei's IRGC-related, including its Hezbollah Division-related and Qods Force-related, projects and/or end-users as there were no suitable foreign-made substitutes for many of them.

936. To obtain other U.S.-origin goods for Hezbollah, the Qods Force, and Regular IRGC Huawei Co., along with Huawei USA, Huawei Device USA, and Futurewei misappropriated trade secrets and intellectual property in the United States from American companies and/or companies with American offices.

937. To source U.S.-origin goods and services, including financial services, to the IRGC's, including Hezbollah's and the Qods Force's, fronts, operatives, and agents, Huawei Co., along with Skycom, Huawei USA, Huawei Device USA, and Futurewei conducted financial transactions through the U.S. and with the use of U.S.-based financial institutions or the U.S. subsidiaries of international financial institutions.

938. Huawei, including Huawei USA, Huawei Device USA, and Futurewei agreed to conceal their unlawful conduct in the U.S. related to its support for Huawei's Iranian business interests, including its contracts with both MTN Irancell and MCI. Thus, Huawei, including its American subsidiaries, destroyed documents in the U.S., deleted electronically stored documents, and directed its employees to make false statements to U.S. governmental authorities and financial institutions.

939. The embargoed United States technology included but not limited to servers, switches, routers, and component parts of cellular network infrastructure.

940. Just about every product that Huawei makes has some American components or software in it, such as microchips, modems, and Google's Android operating system.

941. Public reports indicate Huawei helped funnel software and hardware from U.S. firms including Hewlett-Packard, Microsoft Corp, Symantec Corp, and Novell Inc. to the government of Iran between 2008 and 2014.

942. Huawei Co. also unlawfully arranged a U.S. citizen to provide technology services in Iran for Skycom. Simply put, Huawei could not do the business it did with Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, and thereby cause the transfer of key technology to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, without reaching into the United States to obtain the required U.S.-origin goods and services and to conceal and shield its scheme to do so.

943. Huawei Co.'s regular transfers of communications technologies, including American cell phones, to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, relied upon American contacts, American transactions, American persons, and American service providers, and depended upon Huawei Co. reaching into the United States, or causing agents, cut-outs, or affiliates to reach into the United States, in order to source the premium brand cell phones craved by al-Qaeda and the Taliban at all times after 9/11. On information and belief, from 2005 through present, Huawei Co. regularly reached into the United States to acquire iconic American communication technologies for the Taliban's benefit, including, but not limited to, numerous technological generations, e.g., iPhone 5, iPhone 6, of: (i) Apple's iPhone and iPad, from California, which were among the most popular cell phones in the Middle East after 2008; (ii) Motorola's Two-Way Push-to-Talk Cell Phone, from Illinois, which was widely associated with Hezbollah and its proxies in the Middle East after the broad media coverage of their use during Hezbollah's 2006 attack campaign against Israel; and

(iii) Motorola's Razr Cell Phone, from Illinois, which was one of the most popular cell phones in the Middle East before and after the iPhone.

VII. DEFENDANTS' TRANSACTIONS WITH FRONTS, OPERATIVES, AND AGENTS OF HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, AL-QAEDA, AND THE TALIBAN CAUSED FUNDS, ARMS, LOGISTICAL AID, AND OPERATIONAL SUPPORT TO FLOW THROUGH TO AL-QAEDA AND TALIBAN TERRORISTS AND AIDED THEIR ATTACKS AGAINST AMERICANS IN AFGHANISTAN

A. Hezbollah, The Qods Force, And Regular IRGC Sourced Weapons, Raised Funds, And Obtained Logistical And Operational Support Through Illicit Corporate Transactions In The Telecom, Communications, And IT Sectors

944. As western sanctions clamped down on Iranian terror fronts, Hezbollah, the Qods Force, and Regular IRGC responded by expanding their efforts to obtain funds, purchase weapons, and source operational support through illicit transactions in the U.S., U.A.E., and Iran.

945. In so doing, Hezbollah, the Qods Force, and Regular IRGC relied on transactions with multinational corporations, like MTN Group, ZTE Corp., and Huawei Co., who operated in key sectors for the dual-use technologies that were essential to the IRGC's, including Hezbollah's and the Qods Force's, communications, surveillance, bombmaking, rocket attacks, intelligence gathering, and project management – everything a transnational terrorist group needs to coordinate attacks against Americans in the Middle East.

946. Sadegh Zibakalam, a professor of political science at the University of Tehran, explained to the BBC in 2012 that “[d]uring the past decade Iran has come up with various ways of getting around international sanctions.” BBC News, *Iran Mobile Operator Irancell ‘Secures US Technology’* (June 6, 2012). Per the BBC, Professor Zibakalam “said Iranian companies had been able to source many American ... goods through international markets, especially companies based in Dubai ... He added that international companies have been eager to assist Iran with equipment it needs.” *Id.*

947. Hezbollah, the Qods Force, and Regular IRGC relied upon the use of concealment and corporate covers to illicitly acquire the technology necessary to continue to scale the IRGC Conspiracy. At all relevant times, Hezbollah, the Qods Force, and Regular IRGC operated purpose-built units designed to extract American technology for use by Hezbollah and the Qods Force by coordinating with organized crime and facilitators. Indeed, the IRGC's use of crooked corporations as fronts is consistent with longstanding IRGC terrorist doctrine, which emphasizes the use of mafia-like "buffers," cut-outs, and fraud schemes designed to route value and services without leaving a paper trail: in short, IRGC terrorist tradecraft.

948. It is widely understood globally that illicit transactions that route money or technology to the IRGC inevitably result in its Hezbollah Division and the Qods Force receiving money, technology, or services that it can use in its terrorist enterprise, and vice versa.

949. Scholars who have studied Hezbollah, the Qods Force, and Regular IRGC concur that they benefit from illicit transactions and that the purported distinction between them is largely immaterial when it comes to Iran's terrorist enterprise and support for terrorist proxies. For example, British researcher Ben Smith, who studied Hezbollah, the Qods Force, and Regular IRGC for the House of Commons, identified telecoms as a key area that financially benefits all:

[T]he Revolutionary Guards, have ***large and expanding business interests*** ... The Iranian economy is "marked by a bloated, inefficient state sector". That has allowed the president to appoint allies and old colleagues from the Revolutionary Guard into key positions in the public sector, and to award government contracts to companies owned ***or*** controlled by Guard members, many of which are involved in dual use technology ... ***including telecommunications*** ... The ***al-Quds force is thought to be no less involved in the business world than the rest of the Revolutionary Guard***, and analysts suspect that these growing business interests provide ***clandestine sources of funding to be channelled to overseas groups and individuals, hidden from [] scrutiny*** ...²⁷⁸

²⁷⁸ Ben Smith (International Affairs and Defence Section of the U.K. House of Commons Library), *The Quds Force of the Iranian Revolutionary Guard -- Standard Note: SN/IA/4494*, UK House of Commons Library Standard Note (Oct. 30, 2007) (emphasis added).

950. Prominent media reports also support this conclusion. According to a 2007 report in the *New York Times*, “[s]ome specialists even question whether the Quds Force exists as a formal unit clearly delineated from the rest of the Revolutionary Guard.” Scott Shane, *Iranian Force, Focus of U.S., Still a Mystery*, N.Y. Times (Feb. 17, 2007). As one such Iran specialist, Vali R. Nasr of the Naval Postgraduate School explained to the *Times*, “[i]t could be that anyone with an intelligence role in the Revolutionary Guard is just called Quds.” *Id.*

951. Moreover, any lines between the IRGC and the Qods Force blur when it comes to Iran’s support for Islamist terrorists outside of Iran. As the same *New York Times* report noted in 2007, “[w]hether properly identified as part of the Quds Force or not, members of the Revolutionary Guard mobilized intelligence and paramilitary agents in Lebanon in the 1980s, where they trained the Shiite militia Hezbollah; in Afghanistan, during the anti-Soviet jihad in the 1980s and episodically since then; in the former Yugoslavia, supporting the Bosnian Muslims against Serbian forces; and in other trouble spots.” *Id.*

952. As the Foundation for Defense of Democracies similarly concluded, given the tight nexus between IRGC commercial activity and violence by Iranian proxies, any transaction with IRGC fronts benefits Iran’s terrorist enterprise – even when it does not result in the IRGC or Qods Force directly obtaining any embargoed arms or technology:

IRGC front companies ... have stakes in telecommunications of which Iran is the largest manufacturer in the Middle East. ... Many IRGC projects are military in nature, and the group ***diverts much of the technology and expertise it acquires from Western companies for seemingly innocuous projects to unsavory ends.*** ... Any company that does business in Iran risks becoming an unwitting accomplice to the IRGC’s nefarious activities ... Yet ***even when companies provide services and technologies that cannot be diverted to illicit projects, partnering with the IRGC entails some complicity with its activities.*** In June 2006, [the head of an IRGC-owned company] confirmed in an interview with a

local daily that the *organization's funds finance various national defense projects, including arming and training Hezbollah.*²⁷⁹

B. Defendants Made Illicit Deals With Hezbollah, Qods Force, And Regular IRGC Fronts, Operatives, Agents, And Cut-Outs That Caused Secure American Smartphones, Enterprise Level Servers, Network Computing Technologies, And Weapons To Flow Through The IRGC To Al-Qaeda And The Taliban And Facilitate Terrorist Attacks On Americans in Afghanistan

953. Beginning in 2005, after Hezbollah, the Qods Force, and Regular IRGC had intensified their support of the terrorist campaign in Iraq, MTN Group, ZTE Corp., and Huawei Co. made illicit deals with IRGC, including Hezbollah and the Qods Force, fronts, operatives, agents, cut-outs, and orbits in the telecom, communications, and network computing sectors. Those deals directly benefited MTN Group, MTN Dubai, ZTE Corp., and Huawei Co. and caused tens of millions of dollars' worth of embargoed American technologies to flow into the IRGC's (including Hezbollah's and the Qods Force's) terrorist enterprise each year.

954. Hezbollah, the Qods Force, and Regular IRGC were able to leverage Defendants' insatiable appetite for Iran's telecom market, which was widely understood to represent a unique opportunity. As *The Economist* explained in 2004, "[w]ith a population of some [70 million people] and a mobile-phone penetration rate of below 5%, Iran offers a unique opportunity for telecommunications investors. ... However, the wrangles with ... Turkcell illustrate the difficulties in assessing the political risk associated with trying to enter the Iranian market."²⁸⁰

955. MTN Group, MTN Dubai, ZTE Corp., and Huawei Co. engaged in virtually identical conduct throughout the course of the Conspiracy. Since MTN Group joined the Conspiracy in 2005, MTN Group, MTN Dubai, ZTE Corp., and Huawei Co. have each acted in a

²⁷⁹ Mark Dubowitz and Emanuele Ottolenghi, *The Dangers Of Doing Business With Iran's Revolutionary Guards*, *Forbes* (June 15, 2010) (emphasis added).

²⁸⁰ Economist Intelligence Unit, *Iran: Putting Up The Shutters*, *Bus. Mid. E.* (Sept. 1, 2004).

manner consistent with terrorist operations, and each of them have demonstrated the ability to execute complex financial frauds spanning multiple continents without detection, bearing all the hallmarks of the IRGC's terrorist tradecraft.

956. MTN Group, MTN Dubai, ZTE Corp. and Huawei Co. followed a common tradecraft when pursuing their illicit acquisitions of embargoed American technologies for Hezbollah, the Qods Force, and Regular IRGC.

957. MTN Group's, MTN Dubai's, ZTE Corp.'s, and Huawei Co.'s transactions provided financial, technical, logistical, and operational support to Hezbollah, the Qods Force, and Regular IRGC worth tens of millions of U.S. dollars per Defendant each year, which funds their terrorist proxies including, but not limited to, al-Qaeda (worldwide), and the Taliban, including its Haqqani Network, in Afghanistan.

958. MTN Group, MTN Dubai, ZTE Corp., and Huawei Co. furthered the Conspiracy by ensuring its concealment for years through their rigorous adherence to the core principles of terrorist tradecraft specifically practiced by the IRGC, including its Hezbollah Divisions and Qods Force, while performing "security"-related operations, e.g., Qods Force facilitation of al-Qaeda/Taliban attacks in Afghanistan. Defendants' rigorous adherence to IRGC terrorist tradecraft furthered the Conspiracy because it provided concealment to the fronts, operatives, and illicit transactions that channeled millions through to Hezbollah, the Qods Force, and Regular IRGC and through them, to the IRGC's terrorist proxies worldwide.

959. MTN Group, MTN Dubai, ZTE Corp., and Huawei Co. deployed numerous illicit strategies to covertly route embargoed American smartphones, servers, network computing systems, and the associated technical support services without which their high-end gear was of little value. While the strategies differed over time, each shared a common specific intent: to

cause tens of millions in valuable state-of-the-art American technologies, services, and currency to flow from the United States to Hezbollah, the Qods Force, and Regular IRGC and through them, to the IRGC's Shiite and Sunni terrorist proxies worldwide, in order to sustain the terrorist campaigns in Iraq, Afghanistan, Yemen, Syria, and Europe.

960. Defendants' illicit deals with Hezbollah, the Qods Force, and Regular IRGC fell into three broad categories of deal type: (1) weapons procurement through sham deals; (2) financing through illicit transactions; and (3) operational support obtained through the legitimacy of the companies helping Hezbollah, the Qods Force, and Regular IRGC.

961. Although Defendants' illicit transactions with, and resulting cash flow to, fronts, operatives, and agents for Hezbollah, the Qods Force, and Regular IRGC provided especially valuable assistance for al-Qaeda's and the Taliban's terrorist attacks, the causal nexus was not limited to Iran sanctions violations. Whether or not MTN, ZTE, and Huawei technically violated Iranian sanctions (although they did), their transactions with a counterparty that was openly controlled by terrorists – and which openly diverted the fruits of the transactions to terrorist ends – supplied Hezbollah, the Qods Force, and Regular IRGC, and through them, al-Qaeda and the Taliban, with funds, weapons, weapons components, computers, communications gear, enterprise data management solutions, and essential logistical support upon which the Syndicate relied to commit terrorist attacks against Americans in Afghanistan.

962. Defendants knowingly helped Hezbollah, the Qods Force, and Regular IRGC source hundreds of distinct items of state-of-the-art embargoed American technology that was illicitly acquired within the U.S. and then re-exported to Defendants' respective IRGC-front counterparties, to be given to terrorists. Plaintiffs offer representative examples of the "security" assistance that Defendants provided MTN Irancell and TCI (including MCI).

963. For decades, Hezbollah, the Qods Force, and Regular IRGC have recognized the centrality of cell phones to the modern terrorist. Hezbollah has long widely deployed mobile phones as a tool of terror.

964. MTN Group, MTN Dubai, ZTE Corp., and Huawei Co. deliberately engaged in complex schemes to acquire sensitive American technologies on the black market, and route the “security” assistance to Hezbollah, the Qods Force, and Regular IRGC.

C. Defendants Made Illicit Deals With Hezbollah, Qods Force, And Regular IRGC Fronts, Operatives, Agents, And Cut-Outs That Caused Substantial Funds To Flow Through The IRGC To Al-Qaeda And The Taliban And Facilitated Terrorist Attacks Against Americans In Afghanistan

965. Beginning in 2005, after Hezbollah, the Qods Force, and Regular IRGC had intensified their support of the terrorist campaign in Afghanistan, MTN Group, MTN Dubai, ZTE Corp., and Huawei Co. made illicit deals with IRGC, including Hezbollah and the Qods Force, fronts, operatives, agents, cut-outs, and orbits in the telecom, communications, and network computing sectors. Those deals directly benefited MTN Group, MTN Dubai, ZTE Corp., and Huawei Co. and caused tens of millions of U.S. dollars to flow into the IRGC’s (including Hezbollah’s and the Qods Force’s) terrorist activity each year.

1. Procurement Bribery

966. The IRGC operated one of the most corrupt procurement environments globally.

967. The IRGC’s approach was not out of line with prevailing Iranian corruption practices. As one trade publication explained, “[c]orruption” is [a] [k]ey [c]oncern,” in Iran “[a]nd [w]ill [l]ikely [w]orsen” because “[a]n endemic culture of corruption appears to pervade all areas of society in Iran, presenting a major obstacle for private and foreign-owned

businesses.”²⁸¹ Indeed, “Iran provides a highly conducive environment for corruption to flourish, primarily due to the opaque and complex nature of government, and the convoluted process of completing bureaucratic procedures.”²⁸²

968. Under official IRGC, including Hezbollah and the Qods Force, policy, Hezbollah, the Qods Force, and Regular IRGC follows a mafia-style financial approach under which all IRGC, including Hezbollah and Qods Force, fronts, operatives, agents, cut-outs, and orbits share a percentage of all income they realize with Hezbollah, the Qods Force, and Regular IRGC like how a mafia lieutenant kicks up a portion of his earnings to the mob boss. For example, in 2003, the IRGC issued a directive decreeing that profits realized by IRGC fronts, operatives, and agents must be shared with the broader IRGC organization, i.e., its Hezbollah Division and Qods Force. The IRGC issued this directive as it was ramping up for a long multi-front terrorist campaign against the United States, and the point of the directive was to escalate the flow of funding supporting the IRGC’s terrorist proxies in Iraq and Afghanistan.

969. Hezbollah, the Qods Force, and Regular IRGC have long emphasized weaponizing their control (directly or indirectly) of procurement processes to generate cash flow.

970. Acting through its Hezbollah Division, the IRGC has long counseled its terrorist proxies about the utility of seizing government ministries, state-owned-enterprises, and private commercial businesses in order to convert them into tools of terrorist finance.

971. The IRGC’s Shiite terrorist proxies made this a calling card of IRGC-backed terror, having deployed the strategy in every IRGC-backed terror campaign since the Islamic Revolution in 1979, including Hezbollah’s control of social services in Lebanon, Jaysh al-

²⁸¹ Emerging Monitor Online, *Iran: Major Barriers To Investment* (Feb. 19, 2016), 2016 WLNR 5299681.

²⁸² *Id.*

Mahdi's control of the Iraqi Ministry of Health, and the Houthis' control of certain geographies in Yemen, as three examples.

972. From the perspective of an operative, agent, cut-out, cover, or proxy ally of Hezbollah, the Qods Force, and Regular IRGC, the IRGC's procurement bribery tradecraft usually calls for the following principles:

- (i) for ordinary procurement projects, e.g., a captive ministry purchasing a supply of commodities, the terrorist should extract a bribe or kickback of ten percent or more (and regularly much more), often styled as a *khums* and delivered in cash (U.S. Dollars required) or "free goods";
- (ii) for mega-blockbuster procurement projects, e.g., building the complete nationwide infrastructure for a communications device, the terrorist should extract whatever the terrorist can get, but should not get greedy or let the perfect be the enemy of the good (the terrorist analogue to the maxim "pigs get fat, hogs get slaughtered"); and
- (iii) regardless of project type, the terrorist should follow similar terrorist tradecraft, including, but not limited to, emphasis on concealment and covers.

2. "Free Goods"

973. Hezbollah, the Qods Force, and Regular IRGC have long emphasized manipulation of local and regional black markets as an ideal source of cash flow.

974. The IRGC has long preferred "free goods" bribes as a tool of terrorist finance because "free goods" serve as cash equivalents given the ease of black market access throughout the region, and "free goods" do not leave as large (or any) of a paper trail.

975. Hezbollah, the Qods Force, Regular IRGC, and every IRGC Shiite Terrorist Proxy has deep experience monetizing every conceivable type of "free good" on the black market because every such terrorist group draws most of its members from geographies where black markets have been endemic for decades, including several where certain goods could only be acquired on the black market (e.g., medicine in Syria during the violence).

976. Hezbollah, the Qods Force, and Regular IRGC specifically trained their operatives with respect to terrorist tradecraft concerning cell phones, including, but not limited to, how a terrorist can treat cell phones as cash equivalents to be sold or traded like any other precious commodity, e.g., gold, in support of the Conspiracy.

977. This is important because each Defendant caused thousands, if not tens of thousands, of secure U.S. cell phones, to flow through MTN Irancell and/or TCI to the terrorists.

978. The going rate for a “clean” American cell phone on the black market is a 10X markup. The phones that get busted out into this market are ordinarily priced at around \$200 per phone since the annual contract heavily subsidizes the phone. Thus, black market sellers who flip an ordinary U.S. cell phone on the black market usually earn about \$2,000 per phone.

979. The IRGC’s historic preference for “free goods” as a form of terrorist finance was met by Defendants’ willingness to spend their own money to buy American mobile phones for Hezbollah, the Qods Force, and Regular IRGC. Each Defendant understood that it could curry favor with its IRGC partner by flooding the zone with untraceable American smartphones.

980. On information and belief, Defendants supplied free mobile phones to Hezbollah, the Qods Force, and Regular IRGC because Defendants understood that Hezbollah, the Qods Force, and Regular IRGC, as well as Shiite terrorist proxies like Jaysh al-Mahdi, have long emphasized the exploitation of black markets to derive untraceable terrorist cash flow. Such a view comports with the IRGC’s intense doctrinal focus on concealment as the first virtue of a “security” operative, and the paranoia that IRGC personnel could be detected by the “Great Satan.” Black markets are safely anonymous.

981. Moreover, for decades, corrupt companies in the Middle East have leveraged “free goods” schemes to route bribes to Iran-backed terrorists, and as a result, at all relevant

times there has been a thriving “corruption economy” that roughly traces the “Shiite Crescent” from Iran through Iraq into Syria and terminating in Lebanon. Given the pervasive black markets that flourish here, and throughout the Middle East, Asia, and Africa, so-called “free goods” bribery schemes offer several ideal features for the hardened corporate criminal (or terrorist), including built-in cover if detected (e.g., “we are just a civilian phone company”).

982. Indeed, free goods are an especially potent form of terrorist finance for Hezbollah, the Qods Force, and Regular IRGC because free goods (in the form of technologies like mobile phones) are usually compact, lucrative, odorless, valuable, and easy to unload on the black market. Moreover, free goods offer an enormous tradecraft benefit for terrorists – no paper trail and no electronic or data signature for the Americans to capture.

983. Defendants’ “free goods” to Hezbollah, the Qods Force, and Regular IRGC flowed through to benefit al-Qaeda and the Taliban, including its Haqqani Network, in furtherance of the IRGC’s Conspiracy. Defendants’ provision of free phones to the IRGC caused more frequent, effective, and lethal al-Qaeda and Taliban IED attacks against Americans in Afghanistan by furnishing Hezbollah and the Qods Force with IED bombmaking materials to supply to al-Qaeda and the Taliban, which helped the Syndicate source bomb components and also improved the effectiveness of such Afghan terrorists’ IED attacks against Americans by defeating the U.S. counter-IED technologies with which the IRGC was familiar from Iraq.

3. Exit40

i. Exit40 Was An IRGC Front

984. Hezbollah, the Qods Force, and Regular IRGC have active cells in India, Switzerland, and the U.A.E., and rely upon all three as critical geographies to flow through precious U.S. Dollars and illicitly acquired American technologies to the IRGC’s Hezbollah

Division and Qods Force, to be used to aid the attack campaigns in Iraq, Afghanistan, and elsewhere in furtherance of the IRGC's Conspiracy.

985. Exit40 was a company with letter box offices in the U.A.E., Florida, India, and Switzerland. On information and belief, Exit40 was a front company created by or for Hezbollah and the Qods Force, and owned, controlled, and operated by Hezbollah.

986. On information and belief, Exit40 was purpose-built by Hezbollah and the Qods Force, following IRGC terrorist tradecraft, to serve as a Hezbollah front for illicit fundraising and acquisition of embargoed U.S. technologies including American smartphones and servers.

987. On information and belief, Exit40 supplied the described Security Aid to Hezbollah, the Qods Force, and other IRGC-affiliated terrorists and/or proxies in order to, among other things, aid attacks by the IRGC Syndicate Terrorist Proxies in Afghanistan.

988. On information and belief, Hezbollah and the Qods Force used Exit40 to extract millions of U.S. Dollars and tens of millions worth of American technologies, from inside the United States, through a hub location overseas (e.g., Singapore) before reaching the relevant terrorist cell in Afghanistan, Iraq, Iran, Pakistan, or the U.A.E.

i. MTN Group Knowingly Used Exit40 To Finance Hezbollah And The Qods Force

989. MTN Group and MTN Dubai had a business relationship with Exit40.

990. MTN Group and MTN Dubai have gone to extreme lengths to conceal their business relationship with Exit40. Among other things, MTN Group and MTN Dubai employees have been instructed not to mention Exit40 over the phone or in an email.

991. On information and belief, MTN Group and MTN Dubai personnel discouraged any telephonic or email discussions concerning Exit40 because they knew the relationship with

Exit40 to be illegal, and they believed Exit40 was acting on behalf, directly or indirectly, of Hezbollah, the Qods Force, and Regular IRGC to facilitate attacks against Americans.

992. On information and belief, an operative, employee, agent, or cut-out from MTN Irancell, TCI, the Bonyad Mostazafan, or another IRGC-controlled entity, made MTN Group and MTN Dubai aware that MTN Group and MTN Dubai should use Exit40 in order to help source the U.S. Dollars and American technologies that Hezbollah, the Qods Force, and Regular IRGC needed to deploy in furtherance of the IRGC Conspiracy and attack campaign against Americans in Afghanistan, Iraq, Syria, Yemen, and elsewhere.

993. On information and belief, MTN Group caused the retention of Exit40 by MTN Group, MTN Dubai, or MTN Mauritius, so that Exit40 would serve as MTN Group's, MTN Dubai's, MTN Irancell's and/or TCI's agent or cut-out in order to intentionally route U.S. Dollars and embargoed American technologies through the MTN-related entities, so that some or all of the associated funds or technologies flowed through to Hezbollah, the Qods Force, and Regular IRGC to be deployed in furtherance of the IRGC Conspiracy and attack campaign against Americans in Afghanistan, Iraq, Syria, Yemen, and elsewhere.

994. MTN Group caused MTN Group personnel, MTN Dubai, or an MTN subsidiary, affiliate, agents, cut-out, or business partner to pay millions of U.S. Dollars to Exit40 in order to cause Exit40 to procure the embargoed American technologies identified by Hezbollah, the Qods Force, and Regular IRGC in order to support the IRGC Conspiracy and attacks against Americans in Afghanistan, Iraq, Syria, Yemen, and elsewhere.

995. On information and belief, such transactions by MTN Group and MTN Dubai, or caused by MTN Group and MTN Dubai, routed millions of U.S. Dollars and American

technologies from the United States to the terrorists overseas from on or about 2005 through on or about 2012, which discovery should reveal.

ii. ZTE Corp. Knowingly Used Exit40 To Finance Hezbollah And The Qods Force

996. On information and belief, ZTE Corp. had a business relationship with Exit40. Plaintiffs' belief is based upon, among other things, the nature of the Conspiracy, requirements of IRGC tradecraft, and specific indicia unique to Exit40.

997. ZTE Corp. destroyed vast amounts of data. On information and belief, the data ZTE Corp. destroyed included data relating to Exit40.

998. On information and belief, an operative, employee, agent, or cut-out from MTN Irancell, TCI, the Bonyad Mostazafan, or another IRGC-controlled entity, made ZTE Corp. aware that ZTE Corp., or an affiliate, subsidiary, cut-out, or agent of ZTE Corp., should use Exit40 in order to help source the U.S. Dollars and American technologies that Hezbollah, the Qods Force, and Regular IRGC needed to deploy in furtherance of the IRGC Conspiracy and attack campaign against Americans in Afghanistan, Iraq, Syria, Yemen, and elsewhere.

999. On information and belief, ZTE Corp. caused the retention of Exit40 by either ZTE Corp. or its subsidiary, affiliate, or agent, so that Exit40 would serve as ZTE Corp.'s, MTN Irancell's and/or TCI's agent or cut-out to intentionally route U.S. Dollars and embargoed American technologies through the ZTE-related entities, so that some or all of the associated funds or technologies flowed through to Hezbollah, the Qods Force, and Regular IRGC to be deployed in furtherance of the IRGC Conspiracy and attacks against Americans in Afghanistan, Iraq, Syria, Yemen, and elsewhere.

1000. On information and belief, ZTE Corp. caused ZTE Corp. personnel, or a ZTE subsidiary, affiliate, agents, cut-out, or business partner to pay millions of U.S. Dollars to Exit40

in order to cause Exit40 to procure the embargoed American technologies identified by Hezbollah, the Qods Force, and Regular IRGC in order to support the IRGC Conspiracy and attack campaign against Americans in Afghanistan, Iraq, Syria, Yemen, and elsewhere.

1001. On information and belief, such transactions by ZTE Corp., or caused by ZTE Corp., routed millions of U.S. Dollars and American technologies from the U.S. to the terrorists overseas from on or about 2005 through on or about 2012, which discovery should reveal.

iii. Huawei Co. Knowingly Used Exit40 To Finance Hezbollah And The Qods Force

1002. On information and belief, Huawei Co. had a business relationship with Exit40. Plaintiffs' belief is based upon, among other things, the nature of the Conspiracy, requirements of IRGC tradecraft, and specific indicia unique to Exit40.

1003. Huawei Co. destroyed vast amounts of data. On information and belief, the data Huawei Co. destroyed included data relating to Exit40.

1004. On information and belief, an operative, employee, agent, or cut-out from MTN Irancell, TCI, the Bonyad Mostazafan, or another IRGC-controlled entity, made Huawei Co. aware that Huawei Co., or an affiliate, subsidiary, cut-out, or agent of Huawei Co., should use Exit40 in order to help source the U.S. Dollars and American technologies that Hezbollah, the Qods Force, and Regular IRGC needed to deploy in furtherance of the IRGC Conspiracy and attacks against Americans in Afghanistan, Iraq, Syria, Yemen, and elsewhere.

1005. On information and belief, Huawei Co. caused the retention of Exit40 by either Huawei Co. or another Huawei subsidiary, affiliate, or agents, so that Exit40 would to serve as Huawei Co.'s, MTN Irancell's and/or TCI's agent or cut-out in order to intentionally route U.S. Dollars and embargoed American technologies through the Huawei-related entities, so that some or all of the associated funds or technologies flowed through to Hezbollah, the Qods Force, and

Regular IRGC to be deployed in furtherance of the IRGC Conspiracy and attack campaign against Americans in Afghanistan, Iraq, Syria, Yemen, and elsewhere.

1006. On information and belief, Huawei Co. caused Huawei Co. personnel, or a Huawei subsidiary, affiliate, agents, cut-out, or business partner to pay millions of U.S. Dollars to Exit40 in order to cause Exit40 to procure the embargoed American technologies identified by Hezbollah, the Qods Force, and Regular IRGC in order to support the IRGC Conspiracy and attack campaign against Americans in Afghanistan, Iraq, Syria, Yemen, and elsewhere.

1007. On information and belief, such transactions by Huawei Co., or caused by Huawei Co., routed millions of U.S. Dollars and American technologies from the U.S. to the terrorists overseas from on or about 2005 through on or about 2012, which discovery should reveal.

D. Defendants' Protection Payments To The Taliban Directly Aided Terrorist Attacks On Americans In Afghanistan

1008. Defendants' conduct aided the Taliban's terrorist enterprise. The very nature of the protection-money demands – backed by violent threats conveyed by the same Taliban fighters who were waging an insurgency against the United States – ensured a close connection between the payments and subsequent Taliban attacks on American forces. Such attacks were a necessary consequence of Defendants' payments. When they paid the Taliban protection money, they were not lessening the overall risk of terrorist violence; they were paying the Taliban to redirect its attacks to other targets. One prevailing slogan among private-security contractors in Afghanistan captured that mentality: contractors often said “you want them to fight Big Army [*i.e.*, the U.S. Army] before they fight you.” Defendants' payments accomplished exactly that. They paid the Taliban to attack Coalition forces rather than Defendants' own businesses.

1009. Defendants' protection payments supplied the Taliban with an important stream of revenue it used to finance terrorist attacks against Americans in Afghanistan. Defendants'

protection payments, which created an income stream overseen directly by Quetta leadership, gave the Taliban fungible resources that were vital to its ability to sustain its terrorist enterprise. For that reason, the Commission on Wartime Contracting observed that “diverted funds,” channeled from Western contractors to the Taliban, “directly strengthen the insurgency.”²⁸³

1010. The Taliban institutionalized control of its protection-money revenue. The extraction of protection payments occurred via a highly regulated process designed to ensure that such payments would benefit the broader insurgency. The Taliban’s 2009 Code of Conduct, for example, contained extensive regulations dictating to local field commanders how to collect (and spend) protection money from foreign businesses. As Gretchen Peters has explained, those regulations “literally institutionaliz[ed] how profits earned from organized crime are to be distributed within the command chain.”²⁸⁴ The money flowed both ways – from local commanders up to the Financial Commission for use by the Taliban’s central leadership, and conversely from the leadership back down to local commanders for use in the field. In all cases, the Quetta Shura maintained “final say in all matters of collecting protection money.”²⁸⁵ That discipline allowed protection money collected from all over the country to finance the Taliban’s terrorist machine.

1011. Defendants’ protection payments similarly financed the Haqqani Network. Not only did Defendants fund the Haqqanis directly, but their payments to the Taliban likewise financed Haqqani operations. The Haqqani Network was part of the Taliban and operationally intertwined with Taliban leadership. Thus, according to a declassified 2009 DIA cable, “a large

²⁸³ *CWC Report* at 74.

²⁸⁴ *Crime & Insurgency* at 16.

²⁸⁵ *Id.* at 17.

majority of the Haqqani Network (HQN) funding comes from the Quetta . . . , Pakistan-based Taliban leadership.”²⁸⁶ Per Ms. Peters, the Haqqanis relied on the Taliban organization to “cover operational costs,” with the amount of financing depending on “the funding capacity of the Taliban leadership.”²⁸⁷ The money flow went both ways: payments to the Taliban supported Haqqani attacks, and payments to the Haqqanis supported Taliban attacks.²⁸⁸

1. Defendants’ Cash Protection Payments To The Taliban Directly Funded Al-Qaeda And Taliban, Including Haqqani Network, Attacks Against Americans In Afghanistan

1012. Money supplied the lifeblood of the Taliban insurgency. Financing gave the Taliban the means to recruit and pay terrorist fighters; to acquire weapons and explosives with which to attack Coalition forces; and to maintain the vast operational infrastructure needed to sustain the insurgency. In 2011, it cost the Taliban an estimated \$100-155 million overall to launch attacks and up to \$300 million to “maintain[] the insurgency” generally.²⁸⁹ Those costs ballooned as the insurgency intensified. As a U.N. Security Council report documented, from 2006-2012, the Taliban “managed to finance an ever-increasing number of attacks, reflecting a year-on-year increase in income.”²⁹⁰ The Taliban’s access to financing was vital to its ability to sustain its growing campaign of terrorism against the United States. As one military historian

²⁸⁶ Def. Intelligence Agency, *Afghanistan – Haqqani Network Finances* (Sept. 24, 2009).

²⁸⁷ Gretchen Peters, *Haqqani Network Financing: The Evolution Of An Industry* at 23, Combatting Terrorism Ctr. (July 2012) (“*Haqqani Network Financing*”).

²⁸⁸ *Crime & Insurgency* at 33 (Quetta Shura agreed with the Haqqani Network “to operate alongside each other and to divide the proceeds they earn in some zones where more than one faction operates.”).

²⁸⁹ *U.N. Financing Report* ¶ 34.

²⁹⁰ *Id.*

observed in 2011, “the Taliban’s most significant weapon is not its arms or its ability to mobilize jihadists but the vast sums of money that it seems to have at its disposal.”²⁹¹

1013. Protection payments supplied the Taliban with the means to buy weapons and explosives for use in terrorist attacks. Weapons capable of killing and injuring Americans cost money, and Defendants’ protection payments provided the Taliban with a potent source of funding to cover the cost of its escalating insurgency. As Ms. Peters explained, once companies decided to “pay off insurgents to avoid having [their] projects attacked,” the “insurgents then spen[t] the money they raise[d] to purchase weapons and explosives, which in turn get used to kill American soldiers.”²⁹² Congressman Bill Delahunt was even more succinct. Responding to reports that “U.S.-funded contractors” made “protection payments to the Taliban,” he observed: “That translates into money that the Taliban are using to attack and kill American military personnel, and that’s just simply outrageous.”²⁹³

1014. Even relatively small protection payments had an outsized effect on the Taliban’s terrorist capabilities. Although estimates vary, the Taliban paid many of its rank-and-file fighters about \$100 per month, while mid-level commanders made upwards of \$350 per month. As for many of the IEDs that the Taliban used against Coalition troops, a Pakistani security official estimated that they cost a mere \$100 to make.²⁹⁴ At those rates, even a single protection payment of \$2,000 could finance substantial insurgent violence: it could put ten fighters and a commander in the field for a month and supply them with five IEDs. And Defendants each made

²⁹¹ *Follow The Money*.

²⁹² *Id.* at 31.

²⁹³ Nancy Cordes, *Is Taxpayer Money Funding The Taliban?*, CBS News (Sept. 3, 2009).

²⁹⁴ See Kathy Gannon, *Taliban Gains Money, al-Qaida Finances Recovering*, Assoc. Press (June 20, 2009).

payments that were many orders of magnitude higher. Those payments materially strengthened the Taliban's ability to finance the attacks that killed and injured Plaintiffs.

1015. The effect of protection payments was especially pronounced because they enabled Taliban commanders to pay recruits who fought against the Coalition for financial (rather than ideological) reasons. Taliban commanders typically operated on thin margins and faced constant pressure to raise enough money both to pay fighters and to launch attacks. Protection money was essential to fulfilling both needs: had Defendants refused to pay and cut off that source of revenue, it would have forced Taliban commanders to “decide between paying and feeding [their] troops and launching attacks.”²⁹⁵ Defendants' payments freed Taliban commanders from that choice and enabled them to retain their fighters while continuing with attacks on Coalition forces. As one academic study concluded, protection payments in connection with “development projects and supply contracts” thus “fund[ed] the Taliban and their affiliates” while also “encouraging alienated men to join the insurgency for easy money.”²⁹⁶

1016. This financial link applied to protection payments in all their forms. Due to the Taliban's fundraising apparatus, cash payments to local commanders (or the Taliban Financial Commission) flowed to Taliban leadership for use wherever the insurgents decided to focus their resources. “Salary” payments to Taliban fighters had a similar effect. Not only did those payments relieve financial pressure on local Taliban commanders, but the Taliban extracted a portion of all salary payments received by individual Taliban members – which it likewise routed to the Taliban Financial Commission for the benefit of the nationwide insurgency.

²⁹⁵ *Meyer Interview*.

²⁹⁶ *Economic Impediments* at 80.

1017. Protection payments supplied one of the most quantitatively significant sources of funding for the Taliban. As Secretary of State Hillary Clinton testified before the U.S. Senate Committee on Foreign Relations in 2009: “[O]ne of the major sources of funding for the Taliban is the protection money.”²⁹⁷ The systematic payments effected by large international companies swamped other, smaller-scale protection rackets.

1018. In many areas of Afghanistan, protection payments supplied the single most significant source of funding for insurgent violence.

1019. Protection payments also strengthened the Taliban by allowing it to diversify its income. For an insurgent group subject to crippling international sanctions, diversification was critical: it offered the Taliban a degree of financial resiliency that made it less susceptible to American counterinsurgency efforts. That is why, as the U.S. military began to successfully interdict the Taliban’s other revenue sources (such as narcotics), the Taliban relied increasingly on its protection rackets. That stream of protection money – particularly from larger, well-financed contractors, including Defendants – supplied reliable funding for the insurgency and, almost as importantly, offered insurance against the risk of other funding sources drying up.

1020. Protection payments from Western companies, including Defendants, were also qualitatively material to the Taliban’s terrorist enterprise because of their unique link to the Taliban’s leadership. Unlike funding from other sources (such as smaller businesses) that were more often spent locally, Defendants’ protection payments generally flowed up the Taliban’s organizational chain – or were made directly to top-level Taliban institutions – and supplied

²⁹⁷ *Afghanistan: Assessing The Road Ahead*, Hr’g Before the U.S. Senate Committee on Foreign Relations, S. Hr’g 111-479, at 48 (Dec. 3, 2009) (statement of Hillary Rodham Clinton, Sec’y of State, U.S. State Dep’t) (“S. Hr’g 111-479”).

fungible U.S. dollars available for use by leadership wherever it saw fit.²⁹⁸ In addition, the payments often conferred intelligence benefits on the Taliban by providing details about U.S. government, military, and contractor operations in the area. The Taliban's high-level commanders then used the money and intelligence supplied by Defendants to finance their nationwide terrorist campaign against Americans in Afghanistan.

1021. The Taliban's top-down organizational hierarchy ensured that protection money collected locally in one province helped to finance Taliban operations throughout the country – including in provinces miles away from the site of the payment. That was a core reason why the Taliban moved to institutionalize the collection of protection money from large firms, including Defendants: rather than have commanders spend their protection money locally, the Taliban directed the funds into the group's central coffers for use on a nationwide scale.²⁹⁹ As two Afghanistan scholars documented, such “funds flow[ed] from Taliban-controlled regions up the chain of command to the leadership and then bec[a]me re-dispensed in the form of individual payments” in key provinces throughout Afghanistan.³⁰⁰ Accordingly, Defendants' payments did not merely finance attacks in the immediate areas of their projects; the Taliban's process for redistributing those payments made sure that they financed terrorism throughout Afghanistan.

²⁹⁸ *Id.* ¶ 35 (“[T]he money flowing from “construction and trucking companies, mobile telephone operators, mining companies[,] and aid and development projects goes to the Taliban Financial Commission[,] which answers to the Taliban leadership.”).

²⁹⁹ *See id.*; *Crime & Insurgency* at 17.

³⁰⁰ *Economic Impediments* at 75.

2. Defendants’ “Free Goods” Protection Payments To The Taliban Directly Funded, Armed, And Logistically Supported Al-Qaeda And Taliban, Including Haqqani Network, Attacks Against Americans In Afghanistan

1022. Defendants’ provision of free communications technologies to the Taliban, including its Haqqani Network, as a form of “free goods” protection payments to the terrorists furthered the IRGC’s Conspiracy and provided critical aid to al-Qaeda and the Taliban. At all times, Defendants were aware of the key role that communications technologies played in propagating attacks against Americans by al-Qaeda and its allies. As Eric Schmidt, then Google’s Chair and CEO, and Jared Cohen, then the Director of Google Ideas, noted in 2010:

[F]or all the ... hope abetted by the use of connection technologies, the potential of such technologies to be ... used in dangerous ways should not be underestimated. The world’s most ... violent transnational groups—from al Qaeda ... to the ... Taliban—are effectively using technology to bring on new recruits, terrify local populations, and threaten ... institutions. ... The same encryption technologies used by dissidents ... to hide their private communications and personal data ... are used by [] terrorists... Afghanistan’s telecommunications networks provide a useful case study in how connection technologies can both help and harm a nation. Since U.S. and NATO forces first launched military operations there in 2001, cell-phone access in Afghanistan has grown from zero to 30 percent. ... At the same time, the Taliban have become increasingly savvy about using mobile technology to malicious and deadly effect. Taliban militants have used cell phones to coordinate attacks, threaten local populations, and hold local businesses hostage ... In February 2009, Taliban inmates ... used cell phones to orchestrate a number of coordinated attacks on Afghan ... ministries. In Afghanistan—and Iraq, too—it is not uncommon for insurgents to use cell phones to detonate roadside bombs remotely.³⁰¹

1023. U.S. government reports also alerted Defendants that their protection payments via “free goods” comprised of high-tech communications technologies donated to terrorists also aided Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its

³⁰¹ Eric Schmidt and Jared Cohen, *The Digital Disruption: Connectivity and the Diffusion of Power*, Foreign Affairs, Vol. 89, Issue 6 (Nov. 1, 2010), 2010 WLNR 28476557.

Haqqani Network—all of whom were aided, directly or indirectly, by Defendants’ provision of free goods technology bribes. For example, according to U.S. counterterrorism strategy in 2018:

The technological advances of the past century have created an interconnected world in which it is easier than ever to quickly move people, funding, material, and information across the globe. The backbone of this interconnected system is information technology—largely created and facilitated by the United States Government and private industry—that is increasingly enabling faster transactions of all kinds across the world. Terrorists use these same publicly available technologies to command and control their organizations and to plot attacks, travel, and abuse the global financial system to raise funds and procure weapons, materiel, and basic necessities. Terrorists cannot sustain their operations without these resources. The United States[,] ... [a]round the globe, [] will promote effective enforcement of legislation and policies aimed at protecting ... communication industries.³⁰²

1024. Defendants’ “free goods” deliveries of cell phones, including phones manufactured and/or acquired in the United States, to the Taliban, including its Haqqani Network, also provided another direct cash equivalent, worth approximately \$2,000 per cell phone, to al-Qaeda and the Taliban, including its Haqqani Network. Indeed, at all times, the high-tech cell phones that Defendants illicitly sourced for, and furnished to, the Taliban, as a “free goods” form of protection payment to such terrorists, carried unique value in Afghanistan that ensured their status as one of the single most valuable items any person, including any terrorist, could possess. As the *Sydney Morning Herald* explained, from 2004 onward, “[c]ommunications [were] vastly better” in Afghanistan and, as a result, “Afghans who [could] afford a mobile phone *clutch[ed] them like talismans*; even the Taliban spokesman avail[ed] himself of the best technology: a satellite phone with an automatic message bank that respond[ed] in 10 languages.”³⁰³

³⁰² The White House, *National Strategy for Counterterrorism of the United States of America*, at 15 (Oct. 2018).

³⁰³ Paul McGeough, *In the Shadow of the Guns*, *Sydney Morning Herald* (Aug. 27, 2005), 2005 WLNR 28183961.

1025. Defendants’ “free goods” deliveries of cell phones, including phones manufactured and/or acquired in the United States that Defendants illicitly sourced from America, to the Taliban, including its Haqqani Network, also aided the terrorists’ fundraising campaigns because it gave the Syndicate the technical tools they required to send communications to others requesting (or demanding) payments, including, but not limited to, sending text messages to Afghans soliciting *zakat* contributions and sending messages to companies, including Defendants, soliciting protection payments or, if such terms were already agreed upon, reminding that a payment was due.³⁰⁴

1026. Defendants’ “free goods” deliveries of cell phones, including phones manufactured and/or acquired in the United States that Defendants illicitly sourced from America, to the Taliban, including its Haqqani Network, also provided direct operational and logistical support to al-Qaeda and the Taliban, including its Haqqani Network, by furnishing untraceable, valuable cell phones, which the terrorists could use to communicate with one another to securely coordinate smuggling, transportation, attack plans, and the like.

1027. Defendants’ “free goods” payments of free cell phones to the Taliban, including its Haqqani Network, allowed the Syndicate to maintain its cell phone stockpile without spending as many U.S. Dollars to do so, providing the terrorists a substantial logistical and

³⁰⁴ See, e.g., Rachel Ehrenfeld and John Wood, *Funding Terror; New Technology Terrorists Can Use*, Wash. Times (Mar. 15, 2007) (“We are on the cusp of a new era of terror financing, that of mobile payments or ‘m-payments.’ ... Are Hamas, al Qaeda, Hezbollah and their likes far behind? Soon, every mobile-phone owner will be able to send money, pay bills and make purchases anywhere, anytime. ... Without the implementation of a real-time digital anti-money-laundering compliance framework, the m-payment system is well suited to become the ‘killer application’ for money laundering and terror financing. All you need is a stored value card and m-payments enabled mobile phone and carrier ...[for] members of Hamas and Hezbollah in the United States to send money back to the Middle East, or to each other all over the world ... [including in areas like] Dubai[,] ... a well-known conduit for al Qaeda, Hamas and Hezbollah funding.”), 2007 WLNR 4912741.

financial windfall. In 2006 the *Independent* reported on the common experience, reflected by the example of an Afghan's experience in a key district (Panjawi) in the Taliban's stronghold of Kandahar, that "the Taliban in his district [had] little money but they ha[d] mobile phones."³⁰⁵

1028. Moreover, like its IRGC sponsors, al-Qaeda, the Taliban, and their Syndicate allies in Afghanistan and Pakistan depended upon a vast stockpile of cell phones in order to conduct their terrorist enterprise in Afghanistan, Pakistan, the U.A.E., Iran, and the other key geographies worldwide from which al-Qaeda and the Taliban facilitated terrorist attacks against Americans in Afghanistan. When Defendants provided more than 1,000 "free" cell phones each year, they furnished a key supply of untraceable phones to the terrorists that aided their communications, attack planning, attack operations, logistics, propaganda, smuggling, and travels – every facet of the terrorists' enterprise targeting Americans in Afghanistan.

1029. Al-Qaeda alone, for example, required tens of thousands of untraceable mobile phones each year for the thousands of operatives it deployed in Afghanistan and Pakistan in support of the attacks. For example, in 2002, media accounts noted that "[t]housands of al Qaeda members hiding in Pakistan use[d] cell phones,"³⁰⁶ while, "[i]n Afghanistan, al Qaida were using top-of-the-range cellular phones,"³⁰⁷ both of which trends always endured.

1030. Defendants' "free goods" payments of free cell phones to the Taliban, including its Haqqani Network, also armed al-Qaeda and the Taliban because Defendants' free phones were, themselves, weapons when wielded by Syndicate terrorists. By 2008, while "cell

³⁰⁵ Nelofer Pazira, *Taliban's Terror Tactics Reconquer Afghanistan*, *Independent* on Sunday (UK) (August 20, 2006), 2006 WLNR 17604097.

³⁰⁶ Ralph Joseph, *Chemical Labs Show Al Qaeda Still Active*, *Wash. Times* (Oct. 6, 2002), 2002 WLNR 383410.

³⁰⁷ Phil Hazlewood and Tom Whitehead, *Role of Aircraft Patrolling Skies*, *PA News* (Feb. 13, 2003).

phone[s]” were “[n]othing special in America,” cell phones were “having a profound effect in Afghanistan[,]” where “[m]any Afghans now rel[ied] on cell phones, as [did] Taliban militants.”³⁰⁸ As the *Associated Press* reported at the time, “Taliban” “militant fighters rely on mobile phones to communicate and coordinate their operations.”³⁰⁹

1031. Al-Qaeda and the Taliban also deployed some of Defendants’ “free goods” donations of cell phones as part of their IEDs, using the phones to detonate the bombs that killed Americans in Afghanistan, including on information and belief many Plaintiffs.³¹⁰ By 2005, “[i]t [was] an irony of the digital age that technology ha[d] aided the security forces in detecting and thwarting terrorist operations ... helped terrorists do their evil.”³¹¹ “High-tech communication” technologies, including “[c]ell phones,” in the hands of an al-Qaeda operative after 9/11, constituted a “weapon at the disposal of” the al-Qaeda “terrorist” because “[c]ell phones” “were a key in” Al-Qaeda’s ability to execute “coordinated attack[s],” including “suicide terrorist attack[s],” which attacks were “facilitated by” al-Qaeda’s access to “hi-tech communications”

³⁰⁸ NPR Morning Edition, *Cell Phones Connect Afghans to Rest of World* (Feb. 26, 2008), 2008 WLNR 3764701.

³⁰⁹ Noor Khan, *Taliban Destroy 2 Phone Towers in Southern Afghanistan*, AP DataStream (Mar. 2, 2008).

³¹⁰ See, e.g., AllAfrica.com English, *Terrorists Drew World’s Attention in Madrid* (Apr. 2, 2004) (“Technology has also linked al-Qaeda to the Madrid bombings. Al-Hayat claims that an Islamist source revealed to the newspaper that al-Qaeda trained its fighters in Afghanistan to use mobile phones for setting off explosive devices. The source told al-Hayat that the explosions on the trains were triggered by mobile phones with alarm clocks set to go off at a specific time.”).

³¹¹ James D. Zirin (Member, Council on Foreign Relations), *Terrorism in the Digital Age*, Wash. Times (Dec. 6, 2005), 2005 WLNR 19631068; United News of Bangladesh, *Bomb at Pakistan Shiite Procession Kills 7* (Nov. 24, 2012) (“Officials say Taliban frequently use cellular phones as remote detonators for bomb attacks.”).

technologies, including “[c]ell phones.”³¹² Moreover, when the Syndicate’s IED campaign intensified in 2009-2010, so did its reliance on cell phones, which remained a key detonator.³¹³

1032. Defendants’ “free goods” payments of free cell phones to the Taliban, including its Haqqani Network, also directly facilitated communications between forward deployed al-Qaeda and Taliban, including Haqqani Network, terrorists in Afghanistan and their leadership in Pakistan, which accelerated the pace of the Syndicate’s attack planning and logistics-related communications, causing more al-Qaeda and Taliban attacks against Americans in Afghanistan. Defendants’ free cell phones were vital because, given the nature of communications between Afghanistan and Pakistan, “telecommunication” technologies were “[t]he only way” that “Taliban commanders” at “Taliban headquarters in Pakistan” could communicate with “Taliban” “field commanders in Afghanistan and outside actors in” other countries,³¹⁴ e.g., the IRGC.

³¹² *Id.*

³¹³ See, e.g., CNN Newsroom, *Goes Green; Updates on Major Accident on Missouri's I-44 Crash - Part I*, AP Alert – Environment (Aug. 6, 2010) (CNN reporting that “the Taliban us[ed] IEDs in a deadly campaign of intimidation against Afghan villagers,” the Taliban’s “IEDs” were “the top killers of American and coalition forces,” “often made of cheap materials like fertilizer” and “detonated by” “something as simple as a cell phone”).

³¹⁴ Stewart Bell, *Canada Listening In On Taliban Exchanges*, National Post (May 1, 2007), 2007 WLNR 28591271.

VIII. DEFENDANTS KNEW THAT THEIR TRANSACTIONS WITH HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, AL-QAEDA, AND THE TALIBAN FACILITATED EVERY NODE OF THE CONSPIRACY AND DIRECTLY AIDED TERRORIST ATTACKS AGAINST AMERICANS IN AFGHANISTAN

A. Defendants Knew Their Transactions With Hezbollah, Qods Force, And Regular IRGC Fronts, Operatives, Agents, And Cut-Outs Furthered The IRGC's Conspiracy To Attack Americans In Afghanistan

1033. Defendants knew that their transactions with fronts, operatives, and agents for Hezbollah, the Qods Force, and Regular IRGC financed, armed, and operationally supported Iranian proxy terrorist attacks against Americans in Afghanistan.

1034. Defendants knew that “[c]ompanies doing business in Iran face substantial risks...,” said Sigal Mandelker, Treasury Department undersecretary for terrorism. She added:

.... “deceptive” Iranian transactions that ultimately channel money to terrorists. The Iranian government “uses shell and front companies to conceal its tracks” as part of an elaborate scheme designed to procure cash for the Quds Force of Iran's militant Islamic Revolutionary Guard Corps, which the U.S. designates as a terrorist organization.

1035. By early 2005, it was widely understood in diplomatic, business, and military circles that Hezbollah, the Qods Force, and Regular IRGC had seized control of Iran's telecom, communications, and information technology sectors. Before they transacted with IRGC, including Hezbollah and the Qods Force, fronts, operatives, and agents, Defendants were aware that IRGC, including Hezbollah and the Qods Force, had seized control of these sectors.

1036. Defendants were aware of IRGC's capture of Iran's telecom, communications, and information technology companies in part through their local agents and affiliates, whom Defendants relied upon to keep abreast of Iranian market conditions; these agents (who were subject to Defendants' control and whose knowledge is imputed to Defendants) knew that Hezbollah, the Qods Force, and Regular IRGC controlled Iran's telecom, communications, and information technology sectors and used that control to raise money, obtain weapons, and source

operational support for terrorism. As a general matter, those agents spoke fluent Farsi, had relationships with people throughout Iranian government and industry, and were well-informed about Iranian politics and economics. They could not have remained ignorant of the common understanding that the Iranian telecom, communications, and information technology sectors were controlled by Hezbollah, the Qods Force, and Regular IRGC.

1037. Defendants knew, or recklessly disregarded, that Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban routinely used commercial transactions to raise money and acquire key weapons and weapons components in support of the IRGC's lead terrorist agent, Hezbollah, as well as the IRGC's proxies in Afghanistan, al-Qaeda and the Taliban. As a regional studies professor explained, the commercial center of "Dubai ... maintains crucial avenues for the IRGC ... to generate money" and serves as "the gate to the world for" IRGC front company efforts.³¹⁵

1038. Defendants knew, or recklessly disregarded, that as American sanctions sought to choke off IRGC, including Hezbollah and the Qods Force, access to the global financial system escalated, Hezbollah, the Qods Force, and Regular IRGC responded by using IRGC, including Hezbollah and the Qods Force, front companies and agents in the United Arab Emirates, Iraq, and elsewhere to raise money through criminal enterprise, facilitate terrorist finance through the banking system, and maintain the steady supply of key telecom, communications, and information technologies necessary to continue to prosecute a terrorist campaign against Americans in Afghanistan and elsewhere. Per *Reuters*, the IRGC:

long proved successful in defending [its] economic interests, including in recent years when the sanctions ... effectively exclude[ed] Iran from the global financial and trading system. "Even under very difficult economic circumstances, the

³¹⁵ TRT World (Turkey), *Amid Soleimani Crisis, Iran Threatens to Level Dubai and Israel. But Why?* (Jan. 8, 2020), 2020 WLNR 663153.

funds for the IRGC's activities, whether domestic or overseas, remained intact," said a former official close to the [Iranian] government... As the U.S. and EU sanctions on Iran's oil and finance sectors in 2012 started to bite, the [IRGC] responded by setting up complex operations involving the likes of Dubai ***"The IRGC started to buy hundreds of ... companies around the [U.A.E.] to use as front companies,"*** said a trader involved in ... the oil industry. ***"These companies partnered with some foreign companies to bypass sanctions. Most of the time cash was delivered to a foreign account in a neighbouring country."***³¹⁶

1039. At all relevant times, Defendants understood that the U.S. government believed that IRGC, including Hezbollah and the Qods Force, activities in the U.A.E. supported anti-American terrorism in Afghanistan and Iraq. For example, in 2008, President George W. Bush gave a widely-reported speech to U.A.E. government and business leaders in which he called Iran "the world's leading sponsor of terrorism" and stressed that illicit transactions in the U.A.E. were important to the IRGC's, including Hezbollah's and the Qods Force's, ability to provide "support for Islamist groups and militants in Afghanistan, Iraq, Lebanon and the Palestinian territories."³¹⁷ Press reports concerning President Bush's speech emphasized the U.S. government's efforts "to enforce US sanctions against ... the Qods Force of the IRGC" because "Dubai in particular ha[d] become a financial centre handling substantial Iranian investments which the administration want[ed] to restrict."³¹⁸

1040. From 2005 through 2016, accounts from prominent Western media sources also reported on the direct link between the Iranian telecom, communications, and information technology sectors and Hezbollah, the Qods Force, and Regular IRGC.

³¹⁶ Parisa Hafezi, *RPT-INSIGHT-Iran's Elite Guards to Gain Regional, Economic Power in Post-Sanctions Era*, Reuters News (Jan. 20, 2016) (emphasis added).

³¹⁷ APS Diplomat, *Bush Says Iran Poses Threat To Global Security* (Jan. 14, 2008).

³¹⁸ *Id.*

1041. On information and belief, Defendants were aware of these reports documenting the link between their Iran-related counterparties and Hezbollah, the Qods Force, and Regular IRGC. Each Defendant generally maintained a corporate security group responsible for supervising their global supply chains, doing counterparty diligence, and preventing the theft or diversion of the devices or services they sold, including in the Middle East. As part of such efforts, Defendants' standard practice would have been to conduct basic open-source research on the Iranian telecom market and the mechanics of making telecom deals in Iran – even a modicum of which would have uncovered the above reports discussing IRGC fronts' terrorist ties.³¹⁹

1042. After 2005, Defendants could not have conducted credible due diligence that would have “cleared” their transactions with their counterparties controlled by Hezbollah, the Qods Force, and Regular IRGC. Defendants also knew about the IRGC's, including Hezbollah's and the Qods Force's, control of their business partners based upon the statements set forth in prominent due diligence materials concerning Iran.

1043. MTN's collusion against Turkcell with the conservatives who controlled Hezbollah, the Qods Force, and Regular IRGC fronts responsible for the Irancell contract itself became a notable “red flag” about the highly risky Iranian business environment that Defendants knew of—and ignored. For example, as the *Economist's* flagship due diligence report, the *Economist Intelligence Unit*, explained in June 2005:

There is considerable doubt that [] Turkish investment projects ... will proceed after facing opposition from the new conservative-dominated [Iranian parliament,

³¹⁹ This allegation applies to all Defendants except MTN Irancell. Plaintiffs allege that MTN Irancell relied upon Hezbollah, the Qods Force, and Regular IRGC to conduct diligence on the counterparties with whom MTN Irancell conducted business, and that the IRGC, including Qods Force, fronts, operatives, and agents that owned and managed MTN Irancell would not have approved any significant investment or hire by MTN Irancell if Hezbollah, the Qods Force, and Regular IRGC believed that such proposed deal did not benefit the “security” agenda of the IRGC, including Hezbollah and the Qods Force.

the] Majlis. The Majlis in late 2004 passed a law giving it a veto over foreign investment and in early 2005 ruled that Turkcell ... should reduce its stake in [I]rancell ... to 49% from 70% [and] ... that a majority of Iranian shareholders would have to support any management decisions and that security issues be referred to the intelligence ministry and the Supreme National Security Council. ... The Majlis's opposition to the projects ... is sure to cause nervousness among foreign investors who will see it as calling into question the value of contracts in the Islamic Republic and as a sign of arbitrariness in governance.³²⁰

1044. After MTN had finished off Turkcell and secured the Irancell license from Hezbollah, the Qods Force, and Regular IRGC fronts who controlled Irancell, the *Economist* updated its standard diligence briefing concerning Iran to warn potential investors, including Defendants, against the "High Risk" of doing business with Iranian entities:

Foreign investors are deterred by the nationalist stance of the Majlis towards foreign investment (High Risk). The Majlis in late 2004 passed a law giving it a veto over foreign investment which it has used to ... severely tighten up on the terms of a project by Turkcell ... ***The conditions imposed on Turkcell have seen its bid superseded by a South African company, MTN.*** The episodes caused nervousness among foreign investors who fear that they called into question the value of contracts in [Iran] and indicated arbitrariness in government decision-making. President Mahmoud Ahmadinejad's presidency (until at least 2009, when fresh elections will take place) will ***continue to heighten such concerns.*** ...³²¹

1045. Public statements made by prominent Members of Congress also alerted Defendants to the IRGC's control of the Iranian telecom sector. For example, on February 10, 2011, a bipartisan group of United States Senators and Representatives confirmed the widespread understanding that the IRGC's (and by extension, the Qods Force's) control of the

³²⁰ Economist Intelligence Unit, *Iran Risk: Legal & Regulatory Risk*, Risk Briefing (June 29, 2005), 2005 WLNR 26571496.

³²¹ Economist Intelligence Unit, *Iran Risk: Legal & Regulatory Risk*, Risk Briefing (Nov. 9, 2006) (emphasis added), 2006 WLNR 26677912.

“Iran telecom sector, of which the Iranian Revolutionary Guard Corps owns a significant stake.”³²² These Members’ letter received widespread coverage in the global media.

1046. Pressure campaigns, also known as “private sanctions,” by public interest groups also warned Defendants about the IRGC’s control of the Iran telecom sector. For example, from 2011 through the present, the non-partisan group UANI³²³ has pressured technology and telecom companies to cut ties with IRGC, including Hezbollah and the Qods Force, fronts in order to pressure the Iranian regime to cease its support for anti-American terror and other malign activities in the Middle East. As Ambassador Mark D. Wallace explained in 2012:

[I]n 2011 UANI launched its “Tech and Telecom Campaign” to ***publicly highlight the role of telecommunications companies in Iran and about how their technology was being misused by Iranian government security forces*** ... In so doing, companies were ***directly facilitating the ability of the Iranian regime to wage a campaign of terror*** ... In response to UANI’s campaign, companies like Nokia Siemens Networks and Ericsson agreed to not take on any new business in Iran. ... In today’s integrated business and financial worlds, companies cannot exist in a national vacuum. Any corporation that seeks access to American capital [] is subject to American law, public pressure and American public opinion.³²⁴

1047. Defendants also knew that most of their multinational peers had already chosen to exit ventures in which they participated alongside Iranian entities that could potentially be fronts for Hezbollah, the Qods Force, and Regular IRGC. By 2012, the roster of companies that

³²² Letter from Senators Jim Webb, Jon Kyl, and Richard Burr, and Representatives Ileana Ros Lehtinen and Sue Myrick, *Sens. Webb, Kyl: Sale of U.S. Computer Technology to Chinese Firm Poses Serious Risk Chinese Firm Has History of Illegal Behavior and Ties with the People’s Liberation Army, Taliban and Iranian Revolutionary Guard*, States News Serv. (Feb. 10, 2011).

³²³ UANI is a non-partisan group focused on protecting U.S. national security from the Iranian threat. In 2012, UANI and its Advisory Board included an array of former national security officials from the U.S. U.K., Germany, Israel, and others, including “Graham Allison, Les Gelb and Fouad Ajami, and former government officials including former CIA Director Jim Woolsey, former Homeland Security Advisor Fran Townsend, former Mossad Chief Meir Dagan, former head of the German Intelligence Service Dr. August Hanning, and former head of the United Kingdom’s MI6 Sir Richard Dearlove among many others.” Wallace May 17, 2012, Testimony.

³²⁴ Wallace May 17, 2012, Testimony (emphasis added).

announced an intention to depart Iran included such prominent multinationals as Siemens, Ingersoll Rand, Hitachi, ABB, Porsche, Caterpillar, Komatsu, Bobcat, and others. Huawei was one of the companies to announce its intentions to depart Iran as well, but as alleged herein, Huawei actually did not pull out of the Iranian market. Regardless of whether Defendants' other multinational peers, in fact, exited these Iranian relationships, their public announcement of their intention to do so further alerted Defendants to the extreme risk posed by their continued economic relationships with their Iranian counterparties.

1048. On April 24, 2016, the *Washington Post* published an opinion written by Senator Joseph I. Lieberman, and Amb. Mark D. Wallace in which the authors warned multinational corporations of the severe financial and reputational risk attendant to doing business with a notorious IRGC front, like MTN Irancell, presciently warning Defendants that, “[s]evere risks exist for companies thinking about investing with the ayatollah, including doing business with the wide array of front companies tied to the IRGC, a terrorist organization sanctioned by the United States and the international community.”³²⁵

1049. MTN, from at least 2005 through the present, ZTE, from at least 2008 through at least 2016, and Huawei, from at least 2008 through at least 2014, knowingly structured their transactions to facilitate the IRGC's fundraising, weapons procurement, and operational support from their IRGC-controlled, including Hezbollah- and Qods Force-controlled, counterparties – which Hezbollah, the Qods Force, and Regular IRGC used to support, among other things, al-Qaeda's and the Taliban's terrorist attacks against Americans in Afghanistan. Senior Iranian

³²⁵ Senator Joseph I. Lieberman and Ambassador Mark D. Wallace, *Why Iran Is Arming Up*, Wash. Post (Apr. 24, 2016).

entity officials involved in the Defendants' transactions were avowed, well-known fronts, operatives, and agents for Hezbollah, the Qods Force, and Regular IRGC.

1050. On information and belief, the ZTE, Huawei, and MTN Co-Conspirators extensively collaborated in Iran, by sharing U.S.-origin technology between 2007 and the present day. As early as 2004, MTN Group created a UK-based shell company called Surizon. Surizon's co-owners, its CEO, and "head of international business development" were previously members of MTN Group's founding board, including its General Counsel and the architect of its international expansion.

1051. Surizon's primary products were two software applications: Fast Access to Content, Trends and Statistics ("FACTS") and Network Management System ("NMS"). FACTS was, and still is, an "intelligence system." NMS enables companies to manage and monitor networks like Irancell's and TCI's mix of incompatible US, European, and Chinese-supplied hardware to enable them to supply meaningful data to FACTS.

1052. According to statements by Surizon and multiple MTN and Irancell employees, Surizon's products were, in essence, interfaces and data manipulation scripts wrapped around U.S.-origin technologies created by, *inter alia*, Oracle, Roambi, and BMC. On information and belief, between 2006 and 2007, Surizon and MTN Group 'negotiated' a "21-country deal" to provide "FACTS... across all MTN Group operators."

1053. Surizon and MTN Group customized and deployed FACTS and NMS to each and every one of MTN Group's operating companies, including Sudan, Syria, and Iran, and specifically including the companies whose facilities are integrated into Iran's transnational signals intelligence network.

1054. On information and belief, MTN continues to use and share FACTS and NMS software with third parties, including the Huawei and ZTE Defendants.

1055. The U.S.-origin technologies used by MTN Irancell and supplied by MTN to Huawei and ZTE, and through Huawei and ZTE to TCI, enabled IRGC, including Hezbollah and the Qods Force, to collect surveillance data and deliver intelligence in real time to terrorist agents in the field via smart phone applications. Use of the U.S.-origin technology, as provided by MTN, Huawei, and ZTE, allowed the terrorists to monitor, track, and target Americans. Indeed, the U.S.-origin technologies enabled FACTS users and Iranian third parties to receive text message alerts under user-specified conditions, and to access network data, including interactive maps of subscriber activity using their smart phones, and to query and mine the data its network operations centers collected, via ZTE and Huawei-supplied surveillance hardware (which themselves were also based on U.S.-origin technologies).

1056. On information and belief, MTN provided ZTE, Huawei, and their Iran-based subsidiaries and shell companies with access to Surizon-developed software to realize a partnership in which ZTE and Huawei provided hardware to MTN Irancell and managed its network operations centers, including those co-located with IRGC agents, on a day-to-day basis.

1057. On information and belief, MTN also provided FACTS to TCI and MCI, and to its local Iranian partners, as well as to agents of Hezbollah, the Qods Force, and Regular IRGC. FACTS and NMS enabled the partnership to manage its highly complex multi-vendor network, and to collaborate seamlessly, avoiding serious compatibility issues that would have arisen from using their own in-house applications.

1058. Defendants knew or recklessly disregarded that their corrupt transactions, overseen by a counterparty that Hezbollah, the Qods Force, and Regular IRGC had totally

commandeered, delivered resources directly to Hezbollah, the Qods Force, and Regular IRGC which they provided to al-Qaeda and the Taliban, including its Haqqani Network, in the form of funds, weapons, logistical support, and other aid to commit terrorist attacks against Americans in Afghanistan by al-Qaeda and the Taliban.

1059. The IRGC's control over the Iranian telecom, communications, and computer sector was so complete that by 2004, there was no longer any meaningful distinction between any of the large Iranian telecom, communications, or computer companies and Hezbollah, the Qods Force, and Regular IRGC. Because Hezbollah, the Qods Force, and Regular IRGC had effectively captured the Iranian telecom, communications, and computer sectors and was using such control to fund and arm IRGC proxies that led the al-Qaeda and Taliban attacks against Americans in Afghanistan, transactions with Iranian telecom, communications, and information technology companies directly benefited the Afghanistan Terror Campaign.

1060. Defendants' transactions with their IRGC-controlled, including Qods Force-controlled, Iranian counterparties supplied Hezbollah, the Qods Force, and Regular IRGC, and through such IRGC members, al-Qaeda and the Taliban, including its Haqqani Network, with resources critical to the Syndicate' terrorist operations against Americans in Afghanistan. The IRGC's control over these critical Iranian economic sectors – and the enormous cash flow that came with it, both from normal revenue as well as corrupt payments from foreign companies – was a key source of the IRGC's, including Hezbollah's and the Qods Force's, power.

1061. Indeed, the telecom, communications, and information technology sectors were (and remain) controlled by Hezbollah, the Qods Force, and Regular IRGC precisely because such control allows Hezbollah, the Qods Force, and Regular IRGC to make groups like Hezbollah more effective at attacking the enemies of Iran, both foreign and domestic, through

the substantial funding for Hezbollah, the Qods Force, and Regular IRGC which flows through to IRGC proxies, including al-Qaeda and the Taliban. The IRGC's complete conversion of the telecom, communications, and computer sectors of the Iranian economy as direct tools of terrorism further strengthened the potency of Defendants' illicit transactions as a means of financing, arming, and operationally supporting attacks.

1062. Defendants provided fungible funds to Hezbollah, the Qods Force, and Regular IRGC that inevitably flowed through to, among others, al-Qaeda and the Taliban for attacks against Americans in Afghanistan. As Ambassador Mark D. Wallace explained in 2012, “[a]bsent *economic support from international businesses*, the Iranian regime would *not have the financial wherewithal to ... support terrorism*.”³²⁶

1063. Writing in the *Eurasia Review*, a foreign affairs analyst specializing in Iran explained the tight nexus between economic transactions with the Bonyad Mostazafan and Hezbollah-supported terrorist attacks against Americans in the Middle East:

The question is, where does the revenue go? ... Since US sanctions caused a sharp decline in Iran's official revenues, the regime is facing financial difficulties and cannot fund its proxies to meddle in the region or as the mullahs' call it “expand its strategic scope”. *Iran cannot fund its proxies including Hezbollah, and its multitude of militia forces in Iraq* and Yemen, or its Afghan Fatemiyoun Division and Pakistani Zainebiyoun militias in Syria using its official annual budget. *The millions of dollars used to fund these group must be provided from other financial sources*. ... [B]onyads such as Bonyad-e-Mostazafan, are among the organizations that have *directly assisted the Quds Force in this regard*. Iranian opposition sources have previously stated that the Quds Force receives *most of its funds* from [Bonyads]. ... The US's decision to sanction [Bonyads] will definitely be welcomed by Iranians who are tired of having their *stolen wealth used for terrorism*.³²⁷

³²⁶ Wallace May 17, 2012, Testimony (emphasis added).

³²⁷ Cyrus Yaqubi, *Recently Sanctioned Iran Foundation Is Regime's Slush Fund For Terrorism*, *Eurasia Review* (Jan. 24, 2021) (emphasis added). While Mr. Yaqubi primarily focused on a separate bonyad, his claims apply equally to Bonyad Mostazafan. *See id.* (“[B]onyads such as Bonyad-e-Mostazafan, ... have directly assisted the Quds Force in this regard.”).

1064. Juan C. Zarate, former Deputy National Security Advisor for Combatting Terrorism from 2005 through 2009, previously testified about the key role played by IRGC, including Hezbollah and the Qods Force, front companies in funding and arming anti-American terrorist attacks committed by Iranian terrorist proxy groups:

We have limited tools to address ... terrorism ... And the use of financial power and the power to exclude from the global system is one of our principal if not most effective tools [W]e have to have a comprehensive strategy with the use of all tools of national power. No doubt. But the reality is at the end of the day, these tools are the ones that prove to be most effective.... So we are going to have to, ***if we are honest about what's happening in the international financial commercial order, we are going to have to crack down on Qods Force front companies***..... That's the nature of the Iranian economy in the way that they do business, and the way they have reached precisely what we have cut off that hardened them so much.³²⁸

1065. On April 23, 2012, the Treasury Department announced new sanctions against Iran that recognized that the IRGC's control of the telecommunications sector was inextricably linked with violence, and stated, in part, as follows:

The Order targets ...information and communications technology that facilitates computer or network disruption, monitoring or tracking that could assist in or enable human rights abuses by or on behalf of the ... Government of Iran. Pursuant to this order sanctions were imposed on ... Iran's Islamic Revolutionary Guard Corps (IRGC) ... The IRGC's Guard Cyber Defense Command (GCDC) includes a special department called the Center for Inspecting Organized Crimes (CIOC). ... The IRGC's CIOC has openly admitted that it would forcefully suppress anyone seeking to carry out "cultural operations" against the Islamic Republic via the Internet ... Individuals arrested by the IRGC have been subjected to severe mental and physical abuse"³²⁹

1066. The nexus between Defendants' illicit transactions in the Iranian telecom sector and terrorist violence by Iranian proxies was especially tight. As Ali Alfoneh of the American

³²⁸ Testimony of Juan Zarate, *Sen. Bob Corker Holds a Hearing on Sanctions and the Joint Comprehensive Plan of Action*, SEC Wire (July 31, 2015) (emphasis added).

³²⁹ U.S. Treasury Dep't, *Fact Sheet: New Executive Order Targeting Human Rights Abuses Via Information Technology*, (Apr. 23, 2012).

Enterprise Institute explained, the IRGC pushed its way into the telecom sector mafia-style, and relied upon the funds and technology it acquired through its telecom front companies to fund Hezbollah, the Qods Force, and Regular IRGC operations:

Telecommunications

The *IRGC has also muscled its way into the Iranian telecommunications sector*. In February 2002, Turkish cell phone company Turkcell ... won a bid to inaugurate a second mobile phone network for Iran ... *The Iranian government welcomed Turkcell. That is, Turkcell was welcome until the IRGC complained*. Turkcell would have been in direct competition with IRGC communications technology and electronics firms. The Council of Guardians—an executive body close to the IRGC and the supreme leader—protested that Iranians would have only 30 percent ownership of the new company. Even after the National Bank of Iran bought out foreign investors to achieve a 51 percent Iranian stake, *the IRGC was not satisfied*. The IRGC-operated [IEI] and the [Bonyad Mostazafan]—an independent financial body *traditionally run by a retired IRGC commander and used by the state as a proxy to fund off-the-books IRGC operations*—erected a cascade of legal and practical obstacles leading Turkish investors to retreat from the Iranian market.

The IRGC rooted its rhetoric on Turkcell in national security. ... *the IRGC expects to maintain its dominant position not only on the battlefield, but in civilian sectors as well*. ... Because some of the Iranian economy's most advanced technological undertakings occur under the aegis of the IRGC and within the framework of the Iranian arms industry, the IRGC can monopolize the transfer and adaptation of high technology to civilian applications ... The homepage of [IEI] ... display[s] many consumer goods produced by the arms industry for sale in the Iranian market. The list includes personal computers, scanners, telephone sets and intercoms, mobile phones, and telephone sim cards. These *purchases support ... IRGC operations*³³⁰

1067. As national security analysts Elliot Hen-Tov and Nathan Gonzalez wrote in the *Washington Quarterly* in 2011, Hezbollah, the Qods Force, and Regular IRGC “‘cashed in’ since 2005.”³³¹ They noted the “dramatic increase” in the IRGC’s “economic importance” since 2005:

[T]he Guards [i.e., the IRGC] controlled less than five percent of GDP shortly after the end of the Iran-Iraq War in 1989. Now, they directly or indirectly

³³⁰ Ali Alfoneh, *How Intertwined Are the Revolutionary Guards in Iran's Economy?*, American Enterprise Institute (Oct. 22, 2007) (emphasis added).

³³¹ Elliot Hen-Tov and Nathan Gonzalez, *The Militarization of Post-Khomeini Iran: Praetorianism 2.0*, *Washington Quarterly* (Winter 2011).

oversee ... about 35 percent and growing. ... Prior to 2005, the Guards ... occasionally *used raw power to reverse high-profile tenders in their favor*. One of the *most notable examples* is when it nullified Turkcell's winning bid to operate a second mobile-phone network as part of a consortium [in favor of Defendant MTN]. Upon *pressure by the Guards* and their patrons, the Majles was *forced to change the terms of the deal and revoke Turkcell's majority share in the consortium*. After Turkcell's departure, an Iranian-led consortium *under the ownership of a Guards' subsidiary* [i.e., Defendant MTN Irancell] received the license for the network.³³²

1068. Defendants also helped Hezbollah, the Qods Force, and Regular IRGC arm their terrorist proxies al-Qaeda and the Taliban by providing embargoed dual-use technology from the United States. Defendants' contribution to the terrorist enterprise was essential, as the embargoed American technology that Defendants provided to the IRGC fronts, including its Hezbollah Division and Qods Force, directly improved the efficacy of the IRGC-supported bombs that the Syndicate used to attack Americans in Afghanistan between 2012 and 2017.

1069. The technology Defendants supplied also helped Hezbollah, the Qods Force, and Regular IRGC to logistically support al-Qaeda and Taliban, including Haqqani Network, cells operating in Afghanistan, as well as such group's support cells operating outside of Afghanistan in places like the U.A.E., Pakistan, Iraq, Iran, and other key geographies from which al-Qaeda and the Taliban directly supported the Afghanistan Terror Campaign.

1070. As a result of the foregoing, each time Defendants publicly touted how each had helped improve the technical capabilities of the phones and other network devices supplied to MTN Irancell, TCI, or MCI, MTN, ZTE, and Huawei were also admitting that they were bolstering the communications networks, technologies, and operative phones relied upon by Hezbollah, the Qods Force, and Regular IRGC to sponsor al-Qaeda's and the Taliban's terrorist attacks against Americans in Afghanistan.

³³² *Id.* (emphasis added).

1071. The technology Defendants provided also helped Hezbollah, the Qods Force, and Regular IRGC communicate with one another and with IRGC proxies al-Qaeda and the Taliban, in Afghanistan and throughout the Middle East, by sourcing embargoed dual-use technology from the United States. Indeed, the IRGC's desire to ensure that it could securely communicate with its proxies, including al-Qaeda and the Taliban, was what initially motivated it to instruct MTN, ZTE, and Huawei to obtain the embargoed U.S. technology. And for good reason: for a terrorist alliance seeking to evade the surveillance of the world's greatest military so that it could plan its attacks unmolested, sensitive U.S. communications technology offered an almost impossible-to-overstate communications edge to the terrorists by arming them with state-of-the-art communications and encryption technology.

1072. Defendants' direct provision of "free goods" to Taliban, including Haqqani Network, terrorists in the form of free cell phones directly facilitated attacks against Americans in Afghanistan. The Taliban's, including its Haqqani Network's, ability to access a river of cell phones from the IRGC, including Hezbollah, and from U.S. and international companies -- both of which channels the ZTE Defendants directly facilitated -- keyed the Taliban fundraising and communications campaigns that formed the foundation of the terrorists' victory in Afghanistan in 2021. After Kabul fell, Tim Culpan, a technology columnist for Bloomberg, explained:

[A] few years after the defeat of the U.S. military in 2001, militant Islamists who had once shunned technology ... coordinated their political and operational messages through a ***network of mobile phones***. The decision to incorporate, rather than reject, 21st-century advances became a key factor in the [terrorists'] survival and eventual recovery of [Afghanistan in 2021].

"[The Taliban] moved toward much greater technological sophistication around 2007. It's a sign of the group's ability to adapt and learn, and that's ***one of the reasons they won***," said Vanda Felbab-Brown, senior fellow and director of the Brookings Institution's Armed Non-State Actors Initiative. "One of the things they learned was to focus on communications, and to leave behind the model of the 1990s, which was to move the country away from any kind of modernity." ...

By 2007, ... in the midst of the insurgency against the Americans, the Taliban were using monochrome flip phones from brands like Nokia and Motorola to push propaganda and keep tabs on people. Felbab-Brown recalls visiting Afghanistan at the time, when the movement was sending mass, targeted text messages. They included reminders to pay *zakat* (religious tax) and that the group knew where he lived.

An irony is that this widespread deployment of telecommunications was made possible by U.S. and international companies Before long, Taliban spokesmen fluent in English were regularly and directly updating Western media by text and voice, answering questions and proclaiming victory in battles journalists didn't even know had happened.

At first, the Taliban were seen by foreign powers, and perhaps even by themselves, as a small, fast military force equipped mainly with rifles and RPGs. But with a more modern enemy like the United States and its allies came the need to add psychological operations. "That's where technology is crucial, there's no way around it," says Kamran Bokhari, director of analytical development at the Newlines Institute for Strategy & Policy. "Previously they could do without it, but after 9/11 the world changed."

The Taliban needed to catch up with innovations on the battlefield, and they learned fast. ... And they *weren't just learning from their enemies*. Their fellow jihadists, such as al-Qaeda, ISIS, *and Hezbollah*, had discovered the power of digital technologies to recruit members, threaten opponents, and control messages. The *Taliban benefited from a cross-pollination of the craft* in propaganda and information warfare.

These groups followed the development of technology in the rest of the world. ... [which resulted in] ... the use of more sophisticated handheld devices and faster networks that meant a video could be recorded on a cell phone and e-mailed directly to supporters or international media. The Taliban and their ilk became early adopters ... A key strategy was not only to win battles, but also to shape perceptions of strength and capabilities ... As the US moved into its second decade of occupation, the Taliban kept up a steady drumbeat of messaging across all media, targeting local Afghan forces and governments overseas. The aim was to create the belief that the movement's ascendancy was inevitable and that resistance was futile. The perception helped bring US administrations to the table and may have led to the collapse of the military.³³³

³³³ Tim Culpan, *Technology Fueled the Taliban's Comeback*, NoticiasFinancieras – English (Aug. 23, 2021), 2021 WLNR 27452700

1. Command, Control, Communications, And Intelligence

1073. Command, Control, Communications, and Intelligence (or C3i) are a fundamental cornerstone to all military operations.³³⁴ Without C3i, military operations cannot be synchronized to effect combat operations at a specific time and place. These principles apply not only to legitimate military operations, but are necessary to effect terrorist operations as well. As General George W. Casey explained in 2009: “Technology is [a] double-edged sword. Inexpensive access to information enables entrepreneurs and innovators to *collaborate in developing new technologies* and improving existing ones. Yet our adversaries can *exploit these same technologies to export terror around the globe*.”³³⁵

1074. Defendants’ sourcing of illicit technologies for Hezbollah, the Qods Force, and Regular IRGC enabled the IRGC to accomplish its Revolution in Terrorist Affairs, to devastating effect. “In future operational environments,” General Casey warned, “where the tactical environment and strategic environment will often be seamless, it is the network that will provide the ability to gain and maintain the operational advantage.”³³⁶ When General Casey wrote this, Hezbollah, the Qods Force, and Regular IRGC were already well on their way to becoming the world’s first fully networked terrorist organization, resourced by Defendants’ multinational

³³⁴ LTC Dale E. Fincke, *Principles of Military Communications for C3i*, Army War College School of Advanced Military Studies, (May 20, 1986), <https://tinyurl.com/289buwd7>.

³³⁵ General George W. Casey, Jr., *The Army of the 21st Century*, Army (Oct. 1, 2009), 2009 WLNR 30869494. “The Israeli-Hezbollah conflict also illustrates the potential impact of hybrid threats. Hezbollah employed modern civil technology (secure cell phones, computers and video telecommunications systems) combined with military means (antitank, surface-to-air and antiship missiles, rockets, mortars and unmanned aerial vehicles) and improvised explosive devices in an innovative array of unanticipated patterns.” *Id.*

³³⁶ *Id.*

corporate muscle.³³⁷ Indeed, in 2010, General Casey noted Hezbollah's use of cell phones and secure computers for command and control, which allowed Hezbollah to inflict far higher casualties on their Israeli enemies: "[Hezbollah] had *secure cell phones, used secure computers for command and control and got their message out* on local television, and about 3,000 Hezbollah operatives basically held off 30,000 well-armed, well-equipped Israeli soldiers."³³⁸

1075. **Interoperability.** Defendants also ensured that Hezbollah, the Qods Force, and Regular IRGC realized enormous gains in terrorist effectiveness and lethality based upon the unique interoperability advantages that MTN Group, MTN Dubai, ZTE Corp., and Huawei Co. afforded to the IRGC and its terrorist allies.

1076. **Intelligence.** Defendants also ensured that Hezbollah, the Qods Force, and Regular IRGC achieved a generational improvement in their intelligence collection. As one analyst told the *Christian Science Monitor*, "[m]obile phone networks and how they connect is one of the IRGC's key priorities because it's one of the key tools for opponents," and concluded the IRGC was "improving its connectivity and information-sharing."³³⁹

1077. MTN Group, MTN Dubai, ZTE Corp, and Huawei Co. served as corporate "covers" for Hezbollah, the Qods Force, and Regular IRGC and intentionally structured transactions, supplier relationships, and pricing decisions, among other things, for the specific

³³⁷ Indeed, Hezbollah's leader, Hassan Nasrallah, declared that Hezbollah's control of an independent fiber-optic-based cellular network was its "Number One weapon," and compared attacking it to an attack on his person. Cam Simpson, *Lebanon Deal Boosts Hezbollah; Islamists Gain After Battle Over Secret Fiber-Optic Network*, Wall Street Journal (May 22, 2008) ("[I]t is forbidden to touch [anything] linked to the networks, whether an engineer, a company or a mayor. Touching them is like touching me.").

³³⁸ J.D. Leipold, *CSA Addresses Worldwide Challenges at Brookings Institution*, Defense Department Documents (Feb. 2, 2010), 2010 WLNR 2196129.

³³⁹ Iason Athanasiadis, *How Iranian Dissidents Slip Through Tehran's Airport Dragnet*, Christian Science Monitor (Feb. 8, 2010), 2010 WLNR 2676528.

purpose of illicitly obtaining state-of-the-art American technology, like enterprise level servers. The end goal: transfer the illicitly obtained goods to Hezbollah, the Qods Force, and Regular IRGC for their use in the terrorist campaign against Americans around the world. By serving as corporate “covers” for Hezbollah, the Qods Force, and Regular IRGC each Defendant significantly increased the potency of the scheme, as demonstrated by how long it has endured.

2. Terrorist Finance

1078. **Cash Flow From MTN Irancell and TCI Revenue.** Hezbollah, the Qods Force, and Regular IRGC derived substantial terrorist funding from the billions of dollars in MTN Irancell and TCI-related cash flows, and at least hundreds of millions of dollars annually.

1079. From 2005 through the present, MTN Group’s and MTN Dubai’s illicit transactions with MTN Irancell, the Bonyad Mostazafan, IEI, TCI (including MCI), Exit40, and/or the Akbari Fronts, provided millions, annually, in illicit funds, weapons, and operational support to Hezbollah, the Qods Force, and Regular IRGC, which the IRGC flowed through to its al-Qaeda and the Taliban, including its Haqqani Network, terrorist proxies, who used such resources to attack Americans in Afghanistan, including Plaintiffs and their loved ones.

1080. MTN Group and MTN Dubai significantly increased the cash flowing through MTN Irancell and TCI, and ultimately deployed by Hezbollah, the Qods Force, and Regular IRGC. They did so by illicitly supplying the state-of-the-art American technologies, like servers, to MTN Irancell and TCI, and by extension the IRGC (including Hezbollah and the Qods Force) needed to attack Americans abroad.

1081. By illicitly helping MTN Irancell grow the footprint of its network, MTN Group helped generate new cash flow by connecting more customers to MTN and therefore causing more money to flow through MTN Irancell to Hezbollah, the Qods Force, and Regular IRGC.

1082. As a matter of economic first principles, MTN Group's and MTN Dubai's participation in MTN Irancell caused the latter to become more profitable, because MTN Group was able to bring its networking expertise to the table.

1083. MTN's logic compels this conclusion. According to Gordon Kyomukama, Chief Technical Officer of MTN, "[a]t MTN, extending the footprint of our network and services to ***ensure that we connect more people*** has been and remains a high priority for our company."³⁴⁰

1084. On information and belief, on or about 2012, MTN Group began discussions with one or more components of the U.S. government concerning MTN Group's desire to repatriate hundreds of millions of dollars from MTN Irancell.

1085. The financial, technical, communications, intelligence, and operational support that that MTN Group, MTN Dubai, ZTE Corp., and Huawei Co., and their respective U.S. manufacturers provided to their IRGC-controlled, including Qods Force-controlled, counterparties flowed through to al-Qaeda and the Taliban, including its Haqqani Network, through some channels that were "official" and some that were "off-the-books."

1086. From 2003 through the present, Hezbollah, the Qods Force, and Regular IRGC supplied al-Qaeda and the Taliban – directly to each constituent member – with substantial and regular arms deliveries, financial aid, training, logistical support, communications technology (including secure American mobile phones), safe haven assistance, and aid with narcotics trafficking, each form of aid facilitated their shared terrorist enterprise against America (i.e., the Conspiracy), which the IRGC's Shiite Terrorist Proxies and IRGC's Syndicate Terrorist Proxies used to aid the terrorists' ability to execute the attacks that injured Plaintiffs.

³⁴⁰ Intelsat, *Press Release: Uganda Joins Forces with Intelsat, ITSO and MTN to Accelerate 3G Network Infrastructure Deployment in Rural Areas* (May 4, 2018), <https://tinyurl.com/yzr7jw8c>.

1087. The embargoed dual-use American technology –included the annual funneling of thousands of secure American smartphones, hundreds of millions of U.S. Dollars, and a vast network of logistical and operational support for the Irancell and TCI fronts that MTN Group, MTN Dubai, ZTE Corporation, and Huawei Corporation provided to their counterparties controlled by Hezbollah, the Qods Force, and Regular IRGC. This technology flowed through to the al-Qaeda and Taliban terrorists who committed each attack that injured each Plaintiff, through transfers made by Hezbollah, the Qods Force, and Regular IRGC to al-Qaeda and the Taliban, including its Haqqani Network.

1088. With respect to MTN Group’s, MTN Dubai’s, ZTE Corporation’s, and Huawei Corporation’s “official” transactions with the IRGC, including Hezbollah and Qods Force, front counterparties – which, though notorious, were still illegal – flowed through Hezbollah, the Qods Force, and Regular IRGC into the specific terrorist organizations upon which the IRGC relied to conduct Iranian “security” operations outside of Iran including, but not limited to:

- (i) **Hezbollah’s External Security Organization Budget:** In order to fund, arm, train, equip, and logistically support designated terrorist groups, or forward deployed Hezbollah terrorists, that joined the Conspiracy to attack Americans including, but not limited to:
 - a. Hezbollah’s forward deployed operatives worldwide, including but not limited to, Hezbollah attack planners, bomb makers, logisticians, trainers, attack cells, fundraisers, financiers, propagandists, and videographers, all of whom were regularly forward deployed, under IRGC doctrine, to help commit and plan terrorist attacks alongside local proxy groups (e.g., the Taliban in Afghanistan) wherever Americans were found, including, but not limited to, Iraq, Iran, Lebanon, Syria, Yemen, Bahrain, the U.A.E., Afghanistan;
 - b. The other Hezbollah terrorists who forward deployed to support Iranian terrorist proxies worldwide, including, but not limited to, al-Qaeda and the Taliban.
- (ii) **The Qods Force’s “Security” Budget:** In order to fund, arm, train, equip, and logistically support designated terrorist groups that specifically targeted Americans including, but not limited to:

- a. Hezbollah in Lebanon, Iraq, Syria, Yemen, Afghanistan, Europe, and elsewhere through cooperation with al-Qaeda and the Taliban including its Haqqani Network;
- b. The IRGC Syndicate Terrorist Proxies, in order to facilitate terrorist attacks against Americans worldwide, including, but not limited to, Iraq, Syria, Yemen, Afghanistan, and Europe through cooperation with these FTOs”.

1089. MTN Group, MTN Dubai, ZTE Corp., and Huawei Co., and their respective U.S. manufacturers, Defendants ZTE USA, ZTE TX, Huawei USA, Huawei Device USA, and Skycom, each showered millions in value upon Hezbollah, the Qods Force, and Regular IRGC each year: For MTN, from 2005 until the present; for ZTE, from at least 2008 through at least 2016; and for Huawei, from at least 2008 through at least 2014. Their official transactions flowed through Hezbollah to the terrorist(s) that committed each attack against each Plaintiff.

1090. MTN Group’s, MTN Dubai’s, ZTE Corp.’s, Huawei Co.’s, and their respective U.S. manufacturers, Defendants ZTE USA, ZTE TX, Huawei USA, Huawei Device USA, and Skycom’s covert “off-the-books” assistance to the terrorists was no less important. Hezbollah, the Qods Force, and Regular IRGC provided tens of millions of dollars “off-the-books” to Hezbollah and (through Hezbollah) to local terrorist proxies since Hezbollah’s inception. Defendants’ “off-the-books” financial-, technology-, and services-related transactions with their IRGC, including Hezbollah Division and Qods Force, front counterparties also flowed through the IRGC, its Hezbollah Division and Qods Force, into Hezbollah’s, the Qods Force’s – and ultimately their proxies’ – terrorist budgets in order to fund the attacks committed by al-Qaeda and the Taliban in Afghanistan that injured each Plaintiff. MTN’s, ZTE’s, and Huawei’s illicit transactions with the Bonyad Mostazafan, IEI, MTN Irancell, TCI (including MCI), the Akbari Fronts, and/or Exit40 provided millions in illicit “off-the-books” income, often in U.S. dollars, to Hezbollah, the Qods Force, and Regular IRGC each year, which Hezbollah, the Qods Force, and

Regular IRGC then provided to al-Qaeda and the Taliban so that al-Qaeda and the Taliban could commit each attack that injured each Plaintiff, which they did.

1091. On information and belief, from 2006 through on or about 2010, the IRGC diverted approximately twenty percent (20%) of its net income cash flow from MTN Irancell to the IRGC, Qods Force, and Hezbollah, with each receiving a similar amount each year. At those rates, MTN Irancell annually caused, at least, more than thirty million dollars to flow through the IRGC to the Qods Force, and more than thirty million dollars to Hezbollah. Such cash flows were delivered in regular, predictable amounts, and supported Qods Force and Hezbollah operations, weapons purchases, and personnel costs, among other expenses, in support of anti-American terrorist operations by Qods Force and Hezbollah throughout the Middle East including, but not limited to, Iran, Iraq, Lebanon, and Afghanistan.

1092. On information and belief, after economic sanctions began to hammer the IRGC on or about 2010, the IRGC responded by cutting spending across the board in half, and therefore cut the cash flow through from MTN Irancell to the IRGC, Qods Force, and Hezbollah from twenty percent (20%) to ten percent (10%), with each receiving a similar amount each year. At those rates, MTN Irancell annually caused, at least, more than fifteen million dollars to flow through the IRGC to the Qods Force, and more than fifteen million dollars to Hezbollah. Such cash flows were delivered in regular, predictable amounts, and supported Qods Force and Hezbollah operations, weapons purchases, and personnel costs, among other expenses, in support of anti-American terrorist operations by Qods Force and Hezbollah throughout the Middle East including, but not limited to, Iran, Iraq, Lebanon, Afghanistan, Syria, and Yemen.

1093. **Cash Flow from Terrorist Fundraising Campaigns, Procurement Bribery, Khums, and Financial Management.** Defendants' assistance facilitated terrorist fundraising

campaigns by Hezbollah, the Qods Force, and Regular IRGC that directly supported attacks in Afghanistan and Iraq by channeling resources to the IRGC and its terrorist allies.

1094. Defendants' procurement bribes facilitated terrorist fundraising campaigns by Hezbollah, the Qods Force, and Regular IRGC that directly supported attacks in Afghanistan and Iraq by channeling resources to the IRGC and its terrorist allies.

1095. Defendants' indirect donations (*khums*), meaning the cash flow that Defendants triggered when they paid Hezbollah, the Qods Force, and Regular IRGC (e.g., when they bribed an IRGC cutout in Dubai), facilitated terrorist fundraising campaigns by Hezbollah, the Qods Force, and Regular IRGC that directly supported attacks in Afghanistan and Iraq by channeling resources to the IRGC and its terrorist allies.

1096. Defendants assisted Hezbollah, the Qods Force, and Regular IRGC to revolutionize their financial management capabilities, which meant that the terrorists had more resources upon which to draw for killing Americans.

3. Weapons

1097. **Improvised Explosive Devices (IEDs).** MTN, ZTE, and Huawei also supported the terrorist campaign through their financial support of fronts acting for Hezbollah, the Qods Force, and Regular IRGC which provided them funds, bomb parts, and other necessary material vital to al-Qaeda's and the Taliban's, including its Haqqani Network's, ability to conduct a nationwide IED campaign targeting Americans in Afghanistan. Hezbollah, the Qods Force, and Regular IRGC manufactured and/or sourced key components for the Syndicate's IED attacks, including, but not limited to, the military- and factory-grade embargoed communications technologies, which al-Qaeda and the Taliban used and which were vital to the Syndicate's ability to build the advanced al-Qaeda-designed CAN fertilizer bombs (IEDs and suicide bombs) that benefited from the upgraded communications technologies provided by the IRGC, which in

turn helped al-Qaeda and the Taliban defeat the U.S. countermeasures designed to protect Plaintiffs from al-Qaeda's bomb attacks, and which al-Qaeda and the Taliban used to commit many of the IED attacks that injured Plaintiffs.

1098. MTN's, ZTE's, and Huawei's conduct had an especially tight nexus with al-Qaeda's and the Taliban's, including its Haqqani Network's, ability to execute signature al-Qaeda attacks involving the use of CAN fertilizer bombs, advanced rockets, and hostage-taking. Each IED and advanced rocket that al-Qaeda and the Taliban used to attack and injure each Plaintiff contained, reflected, was reverse-engineered from, and/or was otherwise technologically aided by Hezbollah's, the Qods Force's, and Regular IRGC's use of embargoed American technology. In the case of Huawei, that embargoed American technology was obtained by and through, on information and belief, Huawei's subsidiaries and employees in the U.S., including but not limited to Huawei USA, Huawei Device USA, and Futurewei. In the case of ZTE, that embargoed American technology was obtained by and through, on information and belief, ZTE's subsidiaries and employees in the U.S., including but not limited to ZTE USA and ZTE TX. In the case of MTN, MTN provided such technology pursuant to MTN Group's joint venture with Hezbollah, the Qods Force, and Regular IRGC through MTN Irancell. The embargoed American technology that MTN, ZTE (via ZTE USA and ZTE TX), and Huawei (via Huawei USA, Huawei Device USA, and Futurewei) covertly supplied to Hezbollah, the Qods Force, and Regular IRGC substantially improved the efficacy and lethality of each EFP and rocket used to attack and injure each Plaintiff.

1099. MTN, ZTE, and Huawei also supported the terrorist campaign through their financial support of fronts acting for Hezbollah, the Qods Force, and Regular IRGC, which funded al-Qaeda's and the Taliban's, including its Haqqani Network's, attacks against

Americans in Afghanistan. Hezbollah, the Qods Force, and Regular IRGC manufactured and/or sourced key components for the Syndicate's IED, rocket, and kidnapping attacks, including, but not limited to, the military- and factory-grade embargoed communications technologies, which al-Qaeda and the Taliban used and which were vital to al-Qaeda's and the Taliban's ability to build the advanced al-Qaeda-designed IEDs that al-Qaeda and the Taliban used to commit many IED attacks that injured Plaintiffs.

1100. The IRGC's, al-Qaeda's, and the Taliban's, including its Haqqani Network's, ability to effectively conduct IED attacks directly facilitated their small arms fire attacks against the United States in Afghanistan, including the attacks that killed and injured Plaintiffs. Among other reasons, terrorists in Afghanistan (and elsewhere) commonly used IED threats and placement histories to channel U.S. forces into specific pre-planned ambush sites, sometimes called "kill boxes," in which the terrorists successfully anticipate the travel routes taken by U.S. personnel (the latter, to counter the former's IED threats) and attack the U.S. servicemembers through an ambush involving small arms fire, rather than an IED.

1101. **Small Arms.** Defendants' assistance directly improved the lethality and accuracy of the small arms fire attacks conducted by the IRGC and its proxies, including al-Qaeda and the Taliban, including its Haqqani Network, by allowing the IRGC to purchase more, and more advanced, small arms and associated ammunition, and to provide more, and detailed, training on the advanced small arms tactics needed to successfully kill American servicemembers, including Plaintiffs.

1102. Defendants' assistance also directly aided the IRGC's and its allies' tracking and targeting of American servicemembers in Iraq and Afghanistan through the IRGC's ability to manipulate Defendants' technologies and services, which directly aided al-Qaeda's and the

Taliban's, including its Haqqani Network's, small arms fire attacks against Americans in Afghanistan, including against Plaintiffs.

1103. **Rockets.** Defendants' assistance directly improved the lethality and accuracy of the rockets deployed by Hezbollah, the Qods Force, and Regular IRGC.

2. Recruiting, Fundraising, Strategic Communications, And Disinformation

1104. The IRGC, including its Hezbollah Division and the Qods Force, emphasized the centrality of orchestrated propaganda campaigns to drive recruiting and fundraising, strategic communications to deliver custom messages to custom audiences, and broad disinformation campaigns to conceal the Conspiracy. The terrorists devoted so much time to these efforts for an obvious reason: they played a vital role in furthering the Conspiracy and maximizing the number of Americans the terrorists could kill in Afghanistan, Iraq, and throughout the Middle East. "Based on their extensive reach in the communications economy," according to Ms. Gill, "the IRGC orchestrated a 'comprehensive messaging strategy' using radio and television broadcasts, newspapers, websites, and social media accounts to amplify the message that the Islamic Republic was under attack from the West. Using media infrastructure ... and telecommunications infrastructure ..., the IRGC actively engaged the communications economy in defending the Islamic Republic against the soft war tactics of the West. Gill at 110.

1105. In so doing, the Conspiracy leveraged the explosion of information technologies and computing power since 2000. As the United Nations Office on Drugs and Crime ("UNODC") documented in 2012:

Technology is one of the strategic factors driving the increasing use of the Internet by terrorist organizations and their supporters for a wide range of purposes, including recruitment, financing, propaganda, training, incitement to commit acts of terrorism, and the gathering and dissemination of information for terrorist purposes. While the many benefits of the Internet are self-evident, it may also be used to facilitate communication within terrorist organizations and to

transmit information on, as well as material support for, planned acts of terrorism, all of which require specific technical knowledge for the effective investigation of these offences.³⁴¹

1106. **Recruiting and Fundraising.** Islamist terrorists have widely relied upon antisemitic appeals to raise money, recruit followers, and gain other advantages.

Fourteen years after 9/11, terrorist groups motivated by Islamic extremist ideology, from Al Qaeda to the Islamic State of Iraq and Syria (ISIS), continue to rely on depictions of a Jewish enemy – often combined with violent opposition to the State of Israel – to recruit followers, motivate adherents and draw attention to their cause. Anti-Israel sentiment is not the same as anti-Semitism. However, terrorist groups often link the two, exploiting hatred of Israel to further encourage attacks against Jews worldwide and as an additional means of diverting attention to their cause.³⁴²

1107. Few terrorists are more committed to this strategy than Hezbollah, the Qods Force, and Regular IRGC who have long used baldly antisemitic propaganda as a core part of their terrorist Conspiracy, by spreading the hateful slur that the United States and Israel are part of a Jewish-led cabal seeking to take over Muslim lands.

1108. The IRGC's campaign to spread hateful antisemitic propaganda about Israel, the United States, and people of the Jewish faith were not the idle musings of disorganized radical Islamists blogging out of their parents' basements. These were industrial scale, IRGC- and Hezbollah-administered propaganda campaigns that sought to strengthen the terrorist conspirators' ability to attack Americans worldwide by, among other things: (1) **bolstering terrorist fundraising** by increasing the potency of the terrorists' online fundraising appeals, and thereby drive more dollars to the terrorist campaign; (2) **recruiting more terrorists** by creating the initial touchpoints for new recruits, e.g., a 16-year old watches a splashy Hezbollah video and

³⁴¹ United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* at 1 (Sept. 2012), <https://tinyurl.com/2p8yd643>.

³⁴² Anti-Defamation League, *Anti-Semitism: A Pillar of Islamic Extremist Ideology* at 1 (2015), <https://tinyurl.com/3a6fe4zd>.

decides to join the group; and (3) **enhancing the terrorists' concealment** by flooding the zone with propaganda designed to persuade the population to support the terrorists or, at least, not rat them out to the Americans nearby (almost as good), by portraying a common enemy.

1109. Regular media discussions also specifically alerted Defendants that the IRGC, including its Hezbollah Division and the Qods Force deployed antisemitic propaganda to raise money and recruit terrorists.

1110. In furtherance of the Conspiracy, MTN Group and MTN Dubai were, and remain to this day, one in spirit with the antisemitic terrorist recruiting messaging of the IRGC, including Hezbollah, and the Qods Force, as well as their co-conspirators in Syria (like the Assad regime) and Afghanistan (like al-Qaeda and the Taliban).

1111. *First*, MTN Group and MTN Dubai regularly enabled the creation, uploading, distribution, downloading, and propagation of a near-constant 24/7 river of terrorist recruitment appeals by, among others, the IRGC, Hezbollah, and the Qods Force, through their provision of technical, financial, operational, and personnel support to MTN Irancell and MTN Syria, both of which reinforced the recruiting campaigns.

1112. *Second*, MTN Group and MTN Dubai have never publicly condemned the antisemitic terrorist propaganda they have enabled in Iran (through MTN Irancell), Syria (through MTN Syria), Yemen (through MTN Yemen), and Afghanistan (through MTN Afghanistan). In every country, MTN Group and MTN Dubai facilitated the local MTN subsidiary's direct and indirect assistance to the recruiting campaigns, all of which followed the Hezbollah playbook of using over-the-top bile to raise awareness for recruiting drives, fundraising solicitations, and more.

1113. MTN Group and MTN Dubai were (and remain) one in spirit with the IRGC's, including Hezbollah's and the Qods Force's, antisemitic terrorist recruiting message. Most obviously, MTN Group and MTN Dubai are the but-for cause of the terrorists' ability to spread their recruitment pitches so effectively through the litany of terrorist-enabling services that MTN Group committed every MTN subsidiary and affiliate to provide to all "Iranian Shareholders," i.e., the IRGC, including its Hezbollah Division and the Qods Force, which substantially bolstered the terrorists' antisemitic recruiting and fundraising pitches.

1114. Since 2005, MTN Group and MTN Dubai have broadcast the terrorists' antisemitic recruiting propaganda throughout the Middle East while never once publicly stating that: (a) Israel has a right to exist; (b) bomb attacks against Americans in the Middle East by Iranian proxies are wrongful; or (c) the Holocaust should be remembered. The reason is obvious—MTN agrees with its terrorist business partner: they are one in spirit.³⁴³

1115. **Strategic Communications and Disinformation.** After 9/11, Hezbollah, the Qods Force, and Regular IRGC was keenly aware how an effective strategic communications campaign could directly aid their transnational terrorist Conspiracy. Indeed, no major global terrorist group has a longer, more prolific, or more impactful record of turning effective strategic communications campaigns into new sources of funds, personnel, safehouse, and the litany of other functions that required an ever-growing group of allies and enablers.

³⁴³ A Westlaw News search designed to obtain any media report containing the phrases "MTN Group" or "MTN Dubai" within 100 words of the roots for Israel and antisemitism (Westlaw News "MTN Group" or "MTN Dubai" /100 Israel! Antisem! Holocaust!) reveals approximately 300 documents as responsive hits. Nothing. A comprehensive Google search similarly reveals no statement. MTN Group could, of course, cease broadcasting terrorist propaganda, publicly issue a sweeping defense of Israel's right to exist, and unequivocally condemn bomb attacks supported by Iran. MTN Group's obvious refusal to do so in nearly two decades flies so contrary to global corporate norms one may conclude that MTN Group and the IRGC are one in spirit.

1116. The U.S. military concluded long ago that there was a direct relationship between effective strategic communications and overall probability of success on a given venture. This reflects a recognition, as General George W. Casey, Jr., explained, “Conflicts” will continue to take place under the unblinking scrutiny of the 24-hour media cycle and the World Wide Web.... Adversaries will have many forums in which to disseminate their messages worldwide.”³⁴⁴

1117. Hezbollah, the Qods Force, and Regular IRGC also understood that effective strategic communications were necessary to further the Conspiracy by, among other things, promoting a disinformation campaign designed to conceal the Conspiracy by causing the spread of falsehoods relating to it, and preventing controversies that could expose co-conspirators, incentivize people to exit the Conspiracy, or foreseeably cause a co-conspirator to be financially or logistically unable to continue supporting the Conspiracy, such as a threat that could cause a corporate co-conspirator to lose billions of dollars or cause an individual co-conspirator to lose their life or freedom.

1118. Ms. Gill explained, as published by NATO, that “[t]he Invisible Hand of the IRGC” touched every transaction relating to MTN Irancell, TCI, and their associated IRGC front shareholders and thus “the reliance of the IRGC’s strategic narrative on the communications economy concerns more than explicitly ideological motivations; a distinctly coercive element can also be identified. Beyond their devotion to the Construction Jihad, the Guard relied on the communications economy as a tool of power projection.” Gill at 108. She concluded: “[w]hilst strategic narratives construct the truth, communications economies enable control over

³⁴⁴ General George W. Casey, Jr., *The Army of the 21st Century*, Army (Oct. 1, 2009), 2009 WLNR 30869494.

communicative processes; both reinforce one another to create a hegemonic understanding of reality that supports a political actor's values, interests, or objectives.” *Id.* at 113.

1119. MTN Group coordinated the strategic communications and crisis prevention efforts relevant to the entire terrorist Conspiracy, and managed MTN Irancell-related strategic communications and public branding outside of Iran.

1120. Ever since MTN Group committed itself and every MTN subsidiary and affiliate to the Conspiracy on September 18, 2005, MTN Group pursued an aggressive, more than decade-long, strategic communications campaign to further the Conspiracy.

1121. MTN Group successfully suppressed any leaks, materially negative press reporting, or public sector investigations in the United States, Europe, Africa, or Southeast Asia concerning MTN Group's and MTN Dubai's secret agreement with Hezbollah, the Qods Force, and Regular IRGC until on or about March 28, 2012, when Turkcell sued MTN in federal district court in Washington, D.C., at which time a whistleblower revealed the secret Agreement to the world through Turkcell's lawsuit. On information and belief, MTN Group relied upon effective strategic communications and crisis prevention services to prevent negative information from “leaking” for nearly seven years after the Agreement was signed.

1122. MTN Group's successful communications strategy prevented any major media scandals concerning MTN Group from between 2005 and 2010. Ordinarily, of course, a parent company's brand equity is of no moment in an Anti-Terrorism Act case. But when that parent company is, effectively, the joint venture partner of terrorists, as is the case here, and when the point of the joint venture is to generate cash flow and serve as cover for sourcing illicit weapons parts, then the parent company's brand and reputation are essential.

1123. Simply put, MTN Group began serving as the IRGC's telecommunications- and computing-related financial and logistics agent worldwide in 2005, never stopped doing so, and continues to play the same role today even after the IRGC was designated an FTO. To accomplish that task, MTN Group coordinated a strategy with MTN Dubai to engage in a series of illegal and fraudulent transactions designed to raise money and source key terrorist components from the United States.

1124. When MTN Group and MTN Dubai operated a worldwide campaign to, among other things, illicitly source more than ten thousand (10,000) high-tech American-manufactured smartphones from sellers within the United States to MTN Group and MTN Dubai's crooked agents, employees, and cut-outs worldwide, ***MTN Group and MTN Dubai were acting as a front for Hezbollah and the Qods Force.***

1125. MTN Group's and MTN Dubai's continued service as a terrorist front even after these issues surfaced in litigation in 2012, 2019, and in the instant case. MTN Group and MTN Dubai continue to act as a now notorious front for the IRGC (an FTO), the Qods Force (an FTO), Hezbollah (an FTO), all of whom, as constituent members of the IRGC were, and remain, parties to the Agreement between "MTN" (i.e., all MTN entities worldwide) and the Iranian Shareholders (i.e., all component parts of the IRGC, necessarily including the IRGC's Hezbollah Division and Qods Force). Plainly, they mean to serve as a terrorist front.

1126. In their capacity as long-standing joint venture allies, fundraising partners, and illicit sourcing fronts since 2005, MTN Group and MTN Dubai knew, or were generally aware, that there was a direct, linear, and measurable relationship between MTN Group's and MTN Dubai's public reputation and brand health on the one hand, and the volume of money and illicitly sourced technology that ultimately flowed through to the IRGC, Hezbollah, the Qods

Force, and their terrorist proxies worldwide on the other. On information and belief, such knowledge, or general awareness, extended to, among others: (1) MTN Group's President and CEO; (2) MTN Group's Commercial Director; (3) MTN Group's Board of Directors; (4) MTN Group's in-house counsel and "compliance"³⁴⁵ staff; (5) MTN Group's external advisors; and (6) MTN Dubai's country manager.

1127. The better MTN Group's and MTN Dubai's public reputation and brand health, the more cash to flow through MTN Irancell to the terrorists because, among other reasons: (1) the better MTN Group's and MTN Dubai's brand, the better the sales for MTN Group's joint venture partner, the IRGC, through Irancell; and (2) the easier it was for MTN Group and MTN Dubai to illicitly source the technology demanded by Hezbollah and the Qods Force – especially for the higher-cost items like servers, or unusually large bulk orders of less expensive (but still costly) items, like smartphones. Often, such transactions required that MTN Group, MTN Dubai, and the agents and cut-outs acting on their behalf, transact with suppliers who were more concerned about reputational risk in comparison to the more traditional high-tech black market resellers for things like smartphones.

1128. From 2005 through at least 2011, MTN Group and MTN Dubai pursued a successful strategic communications campaign that prevented any catastrophic public relations scandals in the United States, Europe, Africa, or Southeast Asia concerning MTN Irancell, MTN Group, or any other MTN subsidiary or affiliate that could have undermined MTN Group's and

³⁴⁵ MTN Group and MTN Dubai are actively, and defiantly, aiding multiple Foreign Terrorist Organizations through the ongoing river of cash they are effectively causing to flow to the IRGC, including its Lebanese Hezbollah division and Qods Force, through MTN Irancell, which MTN Group and MTN Dubai refuse to immediately compel to wind down. As such, one may reasonably assume that "compliance" as currently practiced at MTN Group and MTN Dubai is just another euphemism at MTN Group.

MTN Dubai's ability to serve as "cover" most effectively for the Conspiracy's continuing efforts to illicitly source weapons and funds to enable terrorist attacks against Americans globally.

1129. On or about December 2010 or January 2011, MTN Group caused MTN Nigeria to hire Individual 1, a former high-level official in the Obama Administration, ostensibly to give two speeches, for which Individual 1 accepted a \$100,000 speaking fee. On information and belief, MTN Group either wired the \$100,000 to Individual 1's bank account in the United States itself, or MTN Nigeria wired the \$100,000 to Individual 1's bank account at the direction of MTN Group, which thereafter reimbursed MTN Nigeria.

1130. When MTN Group caused MTN Nigeria to pay Individual 1's \$100,000 speaker fee, it was not because MTN Group or MTN Nigeria were interested in Individual 1's speech. Instead, on information and belief, MTN Group caused MTN Nigeria to pay Individual 1, because MTN Group knew that Individual 1 would return to the Obama Administration, and MTN Group intended to induce Individual 1's service as a backdoor channel to the White House.

1131. MTN Group paid Individual 1 because MTN Group knew Individual 1 would be immensely influential within the Obama Administration while it was analyzing, among other things, the geopolitical and public messaging concerns attendant to question of whether to soften the then-existing sanctions, which were crushing the IRGC, and therefore undermining MTN Group's joint venture partner – and, by extension, MTN Group.

1132. MTN Group's retention of Individual 1 in December 2010 and indirect payment (through its captive subsidiary, MTN Nigeria) of \$100,000 to Individual 1 was an act in furtherance of the Conspiracy. On information and belief, MTN Group wired \$100,000 to Individual 1, causing it to be received by Individual 1 inside the United States, hoping that

Individual 1 would, in effect, be on MTN Group's "side" (or at least, willing to take a meeting) when the time was right concerning the sanctions on MTN Group's JV partner, the IRGC.³⁴⁶

B. Defendants Knew That Their Provision Of "Security" "Cooperation" Aid To Hezbollah, The Qods Force, And Regular IRGC Supported Terrorist Attacks Against Americans In Afghanistan By IRGC Proxies Al-Qaeda And The Taliban Because Defendants Knew That "Security" Was An IRGC Euphemism For The IRGC Proxy Attacks Against Americans

1133. By 2005, Defendants' experiences, communications, and awareness of basic facts concerning Iran alerted Defendants to the fact that Iran's "security" was controlled by the IRGC, Hezbollah, and the Qods Force and such "security" was a widely known euphemism for kidnapping and terrorist attacks against Americans by these groups. Defendants knew that their assistance to Hezbollah, the Qods Force, and Regular IRGC furthered the IRGC's support for terrorists and proxies like al-Qaeda and the Taliban, and constituted an agreement to aid anti-American terrorists that was illegal under U.S. law.

1. In-Person IRGC Communications as Terrorist Tradecraft

1134. Under standard principles of IRGC terrorist tradecraft, each of the "Iranian Shareholders," including but not limited to each Defendants' handlers and contacts at the IRGC, including its Hezbollah Division and the Qods Force, communicated to Defendants the core price of doing business with Irancell and TCI: that they would have to aid the "security" agenda of Iran, and in particular, Iran's transnational terrorist logistics enterprise. MTN Group and MTN Dubai's experience negotiating with the IRGC from 2004 through 2005 proves it, and the IRGC,

³⁴⁶ Whether MTN Group's transparent attempt to grease a senior insider worked does not matter. What matters is that MTN Group – more than five (5) years after joining the Conspiracy in 2005 – was still coordinating substantial expenditures of time and money for the obvious purpose of improving the economic climate in which MTN Irancell, and by extension the IRGC, operated, and regularly reaching into the United States to do so.

on information and belief consistently followed the same approach with ZTE and Huawei. As a result, MTN Group, MTN Dubai, ZTE, and Huawei knew the deal.

2. Iranian Constitution

1135. Defendants knew that Iran’s constitution distinguishes “security” from other Iranian governmental functions consistent with what Defendants knew — that “security” in Iran means “terror” against Americans outside of it. Examples drawn from Iran’s constitution include, but are not limited to:

- (i) Preamble: “[T]he Islamic Revolutionary Guards Corps are to be ... responsible ...for fulfilling the *ideological mission of jihad* in God’s way; that is, *extending the sovereignty of God’s law throughout the world* (this is in accordance with the Qur’anic verse ‘Prepare against them whatever force you are able to muster, and strings of horses, striking fear into the enemy of God and your enemy, and others besides them’ [8:60]).”³⁴⁷
- (ii) Article 145: “No foreigner will be accepted into the Army *or security forces* of the country.”
- (iii) Article 172: “Military courts will be established by law to investigate crimes committed in connection with military *or security duties* by members of the Army, the Gendarmerie, the police, and the Islamic Revolution Guards Corps.”

3. Iranian National Security Council

1136. The Iranian National Security Council’s structure ensured Defendants knew that “security” was a euphemism for Iran-backed terrorist campaigns against the United States worldwide. Most obviously, Iran’s National Security Council is responsible for its terrorist agenda, including Iran’s routine deployment of proxies like Hezbollah to coordinate attack campaigns against Americans globally.³⁴⁸

³⁴⁷ The emphasized passages are widely understood, inside Iran and around the world, to refer to the IRGC’s foundational mission of attacking the United States around the world in order to advance the Iranian Islamic Revolution.

³⁴⁸ See, e.g., Ali Reza Nader (Senior International Policy Analyst at RAND Corp.), *Iran Vote is Cause for Optimism*, Realism, Star Tribune (June 19, 2013) (“A 20-year parliamentarian,

4. Hezbollah Structure

1137. Hezbollah's organizational chart also confirmed that Defendants knew that "security" was a euphemism for terror. As the "Hezbollah Division" of the IRGC, Hezbollah is a subordinate branch of the IRGC, and therefore because the IRGC is in charge of "security" in Iran, it necessarily follows that "security" matters in Iran also include Hezbollah and the Qods Force. Moreover, from the 1990s through the present, the structure of Hezbollah's purported "terrorist wing"³⁴⁹ has always been officially and publicly referred to as Hezbollah's "External *Security* Organization."

5. IRGC Doctrine

1138. Unlike nearly every other terrorist group, the IRGC was founded and explicitly committed to anti-American terror as a matter of Iranian national security doctrine targeting the United States (the "Great Satan") for external terrorist attacks in order to advance Iran's Islamic revolution globally. As Dr. Mark Silinsky, a 36-year veteran military intelligence analyst at DOD and an affiliated professor at the University of Haifa, explained in 2019:

The third *major goal* of the IRGC is *combatting Iran's declared enemies, the most reviled of whom are the United States*, Israel, and Saudi Arabia. A leading IRGC-controlled media outlet claims that those three countries "finance terrorists and provide them with weapons." Iranian hatred of the United States is deep and enduring. Early in his adulthood, Khomeini named the United States the "Great Satan," a moniker that endures today. ... Iranian leaders often clamor that the United States has dominated weaker countries for centuries and proclaim that the United States intends to destroy Islam and the Islamic Republic of Iran. In Iran,

Rowhani formerly led Iran's security council, so he has had direct knowledge and/or involvement in Iran's internal repression and external support of terrorist organizations like Hezbollah."), 2013 WLNR 15146323.

³⁴⁹ Like its IRGC overlords, and Iranian terror proxies like Jaysh al-Mahdi, Lebanese Hezbollah maintains a fictional separation between their "terrorist" and "political" wings, but this is just terrorist tradecraft designed to provide concealment for Hezbollah operatives, and there is no meaningful firewall between the two wings.

there are broadcasts, television shows, movies, songs, and video games with the theme of destroying America.³⁵⁰

6. Iran-Focused Scholars

1139. According to a broad consensus of Iran scholars, “security” ordinarily is understood in the Iranian context, by all sides, to refer to IRGC-related terror operations against Americans carried out by the Hezbollah, the Qods Force, and associated terrorist proxies, including, but not limited to:

- (i) Tony Badran, September 2011: “[T]he Qataris also ran their initiative by Tehran, in order to ... assure the Iranians that Syria’s ‘security doctrine’ meaning its policy of support for so-called ‘resistance movements’ sponsored by Iran would remain intact.”³⁵¹
- (ii) Ambassador R. Nicholas Burns, January 2016: “[T]he people who actually run Iran’s security policies, their intelligence networks, their support to the terrorist groups like Hezbollah and Hamas, are in the Iranian Revolutionary Guard Corps. That group of people has a fundamentally more anti-American, cynical, brutal view of the future of Middle East politics.”³⁵²
- (iii) Nakhleh Emile, June 2017: “Iran has supported Sunni and Shia terrorist organizations over the years ... in the service of its national interest. Supporting proxy terrorist groups has been a principle of Iran’s security doctrine for years, especially during the period when Iran was threatened with the possibility of regime change.”³⁵³
- (iv) Dr. Ronen Bergman and Dr. Raz Zimmt, July 2018: “While the Iranian nuclear program isn’t under the IRGC’s command, its security definitely is.”³⁵⁴

³⁵⁰ Dr. Mark Silinsky, *Iran’s Islamic Revolutionary Guard Corps: Its Foreign Policy and Foreign Legion*, Marine Corps Univ., Expeditions with MCUP (Digital Journal) (Jan. 2019) (emphasis added), <https://tinyurl.com/j7s3z77t>.

³⁵¹ Tony Badran (Foundation for Defense of Democracies), *U.S. Human Rights Policy in Iran and Syria*, Congressional Testimony via FDCH (Sept. 22, 2011), 2011 WLNR 24786203. Syria and Iran share a common “security doctrine” dictated by the IRGC.

³⁵² R. Nicholas Burns, *quoted in* Ashish K. Sen, *Dealing with Iran: A Policy of Engagement and Deterrence*, Harvard Belfer Center for Sci. & Int’l Affairs, States News Service, (Jan. 19, 2016).

³⁵³ Nakhleh Emile, *Aligning With Iran Necessary to Combat Sunni Extremism*, Iran Times Int’l (June 9, 2017), 2017 WLNR 23277897.

³⁵⁴ Dr. Ronen Bergman and Dr. Raz Zimmt, *Israel’s Most Dangerous Enemy: Who Are You, Hajj, Qasem Soleimani?*, Yedioth Ahronoth (Israel) (July 3, 2018), 2018 WLNR 20323696.

- (v) Seth Frantzman, July 2020: “Iran said it hoped Iraq would play a greater role in regional security, apparently meaning helping Iran work with Syria and perhaps be a conduit for Iran’s weapons trafficking to Syria. Iran has sent ballistic missiles to Iraq in 2018 and 2019 and trafficking precision guided munitions via Iraq’s Al-Qaim border area with Syria. Iraq has recently tried to replace some units on the border to make the border more secure. Regional security, for Iran, means regional Iranian hegemony. Iraq is Iran’s ‘near abroad’ in this equation. The pressure on Kadhimi was intense during the recent visit and Iran showed it means business in terms of pressuring the US to leave Iraq.”³⁵⁵
- (vi) Ariane Tabatabai, November 2020: “[Qassem] Soleimani and [Mohsen] Fakhrizadeh,” the “head of research and innovation at Iran’s Ministry of Defense,” “were the architects of two pillars of Iran’s security policy: its proxy and nuclear programs ... Both helped create the infrastructure and develop the programs. But their deaths won’t lead to a fundamental change, as institutions will continue the projects.”³⁵⁶

7. Terrorist Statements

1140. Public statements by the IRGC, Hezbollah, and the Qods Force also alerted Defendants that “security” was a code word for anti-American terror operations by the IRGC, Hezbollah, and the Qods Force, including, but not limited to:

- (i) BBC, July 2013: “Iran’s MP on security and foreign affairs denounce[d] an EU decision to include Hezbollah military wing in the list of terrorist organizations.”³⁵⁷
- (ii) Fars News Agency (Iran), February 2014: “An Iranian deputy foreign minister blasted Washington for raising baseless allegations against Tehran, and said the US which supports terrorist groups with financial, political and arms aids cannot accuse others of advocating terrorism. ... ‘The Lebanese Hezbollah is strongly fighting terrorism in support of the country’s security and stability,’ the Iranian official added.”³⁵⁸
- (iii) IRIB World Service (Iran), March 2016: “Iran says a decision by Persian Gulf Arab states to brand Lebanon’s Hezbollah as a terrorist group is a ‘new mistake’ that will undermine peace in the region and unity in Lebanon. ... ‘Those who call Hezbollah

³⁵⁵ Seth J. Frantzman, *Iran’s Maximum Pressure on Iraq to Remove US Forces*, Jpost.com (Jerusalem Post online) (July 22, 2020), 2020 WLNR 20379547.

³⁵⁶ Quoted in *Arkansas Democrat Gazette, Iran Claims Israel, U.S. Linked To Slaying Of Key Nuclear Scientist* (Nov. 28, 2020), 2020 WLNR 34141033.

³⁵⁷ BBC Int’l Reports (Central Asia), *Programme Summary of Iranian Gorgan Radio News 1600 gmt 24 Jul 13* (July 25, 2013).

³⁵⁸ Fars News, *Iran Raps US Double-Standard Policy Towards Terrorism* (Feb. 12, 2014).

terrorists, have intentionally or unintentionally targeted the unity and security of Lebanon,' Iran's Deputy Foreign Minister Hossein Amir-Abdollahian said.”³⁵⁹

- (iv) Naharnet (Lebanon), March 2016: “A top Iranian security official ... hailed ... ‘Hizbullah has played a key role in ... protecting Lebanon’s security,’ said Ali Shamkhani, the head of the Supreme National Security Council of Iran.”³⁶⁰
- (v) Seth Frantzman, July 2020: “The Ayatollah stressed that while Iran does not interfere in Iraq, it is the ‘corrupt’ Americans who are interfering in Iraq and who only sow destruction in the region. ... [Iraqi Prime Minister] Kadhimi also met with Ali Shamkhani, the head of the Supreme National Security Council. Shamkhani has visited Iraq earlier this year to pressure Iraq to expel US forces. ... Shamkhani's meeting with Kadhimi was meant to be yet another piece of Iran’s maximum pressure to get US forces out of Iraq. Shamkhani said the Us was ‘evil’ and that it was a ‘malicious, terrorist’ element in Iraq that was leading to insecurity.”³⁶¹

8. Iran-Related “Security” Media Coverage

1141. Regular media discussions also specifically alerted Defendants that “security” was a code word for anti-American terror operations by the IRGC, Hezbollah, and the Qods Force, including, but not limited to:

- (i) Denver Rocky Mountain News, April 1992: “Mughniyeh, chief of security for Hezbollah, the Iranian-sponsored [group], and head of its terrorist arm, Islamic Jihad (Holy War).”³⁶²
- (ii) San Francisco Chronicle, September 2001: “Arranges security for meeting between bin Laden and [] Mughniyeh, security chief for the Iran-sponsored ... Hezbollah.”³⁶³
- (iii) Washington Post, November 2001: “Iran’s foreign and security policies ... back terrorist groups such as Hezbollah ... [T]he head of Iran's judiciary[] recently summed up the view of this wing of the government: ‘Our national interests lie with antagonizing the

³⁵⁹ IRIB World Service (Iran), *[P]GCC Branding of Hezbollah as Terrorist a New Mistake: Iran* (Mar. 3, 2016), 2016 WLNR 6748676.

³⁶⁰ Naharnet (Lebanon), *Iran: Hizbullah Played Key Role in Eradicating Terror in Syria, Protecting Lebanon* (Mar. 17, 2016), 2016 WLNR 8288436.

³⁶¹ Seth J. Frantzman, *Iran’s Maximum Pressure on Iraq to Remove US Forces*, Jpost.com (Jerusalem Post online) (July 22, 2020), 2020 WLNR 20379547.

³⁶² Holger Jensen, *Sanctions Target Libya, Ignore Other Terrorist Regimes*, Denver Rocky Mountain News (Apr. 16, 1992), 1992 WLNR 425546.

³⁶³ Lance Williams and Erin McCormick, *Bin Laden’s Man in Silicon Valley*, San Francisco Chron. (Sept. 21, 2001).

Great Satan,' he stated. ... It would be a mistake for the Bush administration to warm relations without serious progress in reining in Iran's ... terrorist links."³⁶⁴

- (iv) Jerusalem Post, June 2002: "Once in southern Lebanon, the 1992 Palestinian deportees, like Jenin Islamic Jihad leader Sheikh Bessam Sa'adi learned bomb-making and terror techniques from Hizbullah militants and Iranian security agents."³⁶⁵
- (v) Boston Herald, March 2004: "All this would be news for Iranians and specialists were it not for [the] fact[] [that] Iran's security agencies ... are the biggest backers of terrorism in the Middle East, notably through ... Hezbollah...."³⁶⁶
- (vi) Newsweek, June 2004: "While the link to Iran has been publicly known for some time, the 9/11 commission has uncovered evidence that in the mid-1990s Osama bin Laden cast aside religious differences with the Iranians and arranged to have his terror operatives conduct training in explosives and security at Iranian-backed camps run by Hizbullah in Lebanon."³⁶⁷
- (vii) Express on Sunday, March 2005: "[T]he terrorist group Hezbollah and [] Iranian security chiefs ... are key sponsors of international terrorism."³⁶⁸
- (viii) AP Worldstream, August 2006: "State Department spokesman Sean McCormack ... denounced Iran as a supporter of terror groups in defiance of U.N. resolution. That support, he said, was 'an integral part' of Iran's foreign and national security policy."³⁶⁹
- (ix) Khaleej Times, September 2009: "The Middle East Times reported ... that the [U.S.] was stepping up scrutiny of Iranian security and military personnel in the Lebanese communities of Latin America. ... US officials said that in addition to boosting rates of recruitment, Hezbollah agents, supported by Iran, are using very effective routes to smuggle drug profits to the Middle East to aid anti-US counterparts ..."³⁷⁰
- (x) Australian, April 2010: "An ASIO assessment included in the [Australian] federal government's recent counter-terrorism white paper drew attention to the presence in Australia of the Lebanese Hezbollah External Security Organisation (ESO), an Iranian-

³⁶⁴ Washington Post (Op-Ed), *The Irony of Iran* (Nov. 11, 2001).

³⁶⁵ Matthew Gutman, *Packing Up Our Troubles*, Jerusalem Post (June 28, 2002).

³⁶⁶ Boston Herald (Op-Ed), *Taking First Steps in Iran* (Mar. 21, 2004).

³⁶⁷ Michael Isikoff and Mark Hosenball, *Terror Watch: Friends of Al Qaeda*, Newsweek Web Exclusives (June 16, 2004), 2004 WLNR 3641416.

³⁶⁸ Tim Shipman, *How Real is Terror Threat to Britain?*, Express on Sunday (Mar. 6, 2005).

³⁶⁹ Barry Schweid, *U.S. Foresees Further Defiance By Iran To U.N. Demands On Uranium Enrichment*, AP Worldstream (Aug. 8, 2006).

³⁷⁰ Khaleej Times, *The Enemy at the Gates* (Sept. 27, 2009), 2009 WLNR 19020314.

sponsored group described on the federal government's national security website as 'among the best-organised terrorist networks in the world' ... ASIO pinpointed ESO as a group 'with a long history of engaging in terrorist acts.'"³⁷¹

- (xi) American Forces Press Service, April 2010: "Defense officials have described the security threats posed by Iranian proxies operating in the Middle East -- Hamas in Gaza and Hezbollah in Lebanon -- which the United States and Israel consider terrorist organizations."³⁷²
- (xii) Reuters, October 2017: "The Revolutionary Guards (IRGC) are Iran's most powerful internal and external security force."³⁷³

9. "Security" Euphemism-Related Media Coverage

1142. Defendants could not possibly have missed the meaning of "security" when they acted in furtherance of the Conspiracy because decades of media, television, and film events across a broad array of cultures, religions, and languages in the U.S., Europe, the Middle East, and Africa, where Defendants' employees and agents live and work, alerted Defendants that "security" was a famously common euphemism for "terrorism," including, but not limited to:

- (i) Miami Herald, July 1992: "[T]he FMLN has created what the government calls 'terror squads' euphemistically named 'security commissions.'"³⁷⁴
- (ii) Journal of Commerce, November 2002: "The Maritime Transportation Security Act gives us a new euphemism. Inside the Beltway, a 'terrorist attack' is now a 'transportation security incident.'"³⁷⁵
- (iii) Aberdeen American News, June 2004: "'On the roller coaster ride that Iraq has become, ...[w]hat's euphemistically referred to as 'security concerns' ... would be referred to as violent, bloody terrorism in most other parts of the world.'"³⁷⁶

³⁷¹ Australian, *Iranian Embassy 'Spying on Activist Students'* (Apr. 6, 2010).

³⁷² John J. Kruzell, *Gates Satisfied with U.S. Planning to Counter Iran*, Am. Forces Press Serv., Def. Dep't Documents (Apr. 27, 2010), 2010 WLNR 8757413.

³⁷³ Reuters, *Iran Warns US Against Imposing Further Sanctions* (Oct. 8, 2017).

³⁷⁴ Miami Herald, *Peace on a Razor's Edge* (July 30, 1992), 1992 WLNR 2253569.

³⁷⁵ R. G. Edmonson, *Washington View*, J. of Commerce (Nov. 18, 2002), 2002 WLNR 1291549.

³⁷⁶ Aberdeen Am. News, *U.N. Vote Brings Glimmer of Hope* (June 10, 2004).

- (iv) Jerusalem Post, August 2004: ““The term ‘security prisoners’ is ... a euphemism for ideologically motivated murderers convicted of terrorist activities against Israelis.””³⁷⁷
- (v) Toronto Star, May 2005: “In an extraordinary trip to Abu Ghraib prison ... she encounters the now-notorious U.S. Army General Janis Karpinski, who tells her that ‘security detainees,’ the euphemism for terrorism suspects held by the U.S. forces, are ‘relaxed, comfortable, and had everything they need.’”³⁷⁸
- (vi) Times of India, November 2006: “There are an infinity of angles at which Anglo-Pakistani relations fall but there is only one - security - at which they stand. The ‘S’ word is a euphemism for the ‘T’ word. Terrorism, as sponsored by Pakistan.”³⁷⁹
- (vii) New American, April 2008: “Lieutenant General Keith Dayton, the Bush administration’s Security Coordinator for Palestine, testified ... on the supposed need to fund President Abbas’ ‘security forces,’ a euphemism for the collection of terrorist thugs from the al-Aqsa Martyrs Brigades, Islamic Jihad, ... and [] other ... militias.”³⁸⁰
- (viii) Birmingham Post, October 2008: “[A]n event ... sought to consider ‘security and community cohesion’ a euphemism for extremism and terrorism, natch).”³⁸¹
- (ix) BBC International Reports (Latin America), October 2013: “Although paramilitary forces could serve the interests of the State, its members act as mercenaries, assault squads, thugs, and private security groups, the latter a euphemism for terrorists.”³⁸²
- (x) Electronic Intifada (Palestine), August 2021: “The term ‘ISF’ – which stands for ‘Israeli security forces’ – is a total misnomer and euphemism for occupation forces who provide anything but ‘security.’ Their job, rather, is to terrorize and repress.”³⁸³

³⁷⁷ Efraim Inbar (Bar-Ilan University), *Let Them Starve*, Jerusalem Post (Aug. 22, 2004).

³⁷⁸ Olivia Ward, *Finding Dignity Amid the Chaos; Iraq Journal*, Toronto Star (May 22, 2005).

³⁷⁹ Rashmee R. Lal, *TomKat Nuptials Like Blair-Mush Compact*, Times of India (Nov. 19, 2006).

³⁸⁰ William F. Jasper, *A Bad Investment*, New American (Apr. 28, 2008).

³⁸¹ Chris Allen, *Freedom of Expression is Built on the Right to Offend*, Birmingham Post (UK) (Oct. 16, 2008), 2008 WLNR 19647906. “Natch” means “naturally; as may be expected.”

³⁸² BBC Int’l Reports (Latin America), *Costa Rican Daily Warns Caution Over Alleged Presence of Paramilitary Group* (Oct. 3, 2013).

³⁸³ Electronic Intifada (Palestine), *Video Shows Israeli Shooting That Killed 11-Year-Old Boy* (Aug. 4, 2021), 2021 WLNR 25165762. Plaintiffs categorically reject the antisemitic bile displayed in this quote and offer it merely to show the widespread euphemistic use of “security.”

- (xi) *Canada Stockwatch*, September 2014: “[I]n the ... Congo ... a ... ‘security incident[]’ ... is one of several euphemisms for an ‘act of terror ...’”³⁸⁴

10. Each Defendant’s Consciousness of Guilt

1143. The conduct of MTN Group, MTN Dubai, MTN Group’s President and CEO, MTN Group’s Commercial Director, ZTE Corporation, ZTE USA’s in-house attorney, Huawei Co., Huawei Co.’s CFO, and others compels the conclusion that each Defendant knew that “security” was a euphemism for the external terror operations of Hezbollah, the Qods Force, and Regular IRGC. Each Defendant manifested obvious **consciousness of guilt** concerning their relationship with the Iranian Shareholders:

- (i) **MTN Group’s CEO** concealed the secret agreement from MTN Group’s shareholders, Board of Directors, outside counsel, auditors, as well as various governments including, on information and belief, the U.S. government and the South African government.
- (ii) **ZTE Corp.**, and its internal legal department, also showed consciousness of guilt because it created internal memoranda intended to guide a company-wide scheme to evade U.S. sanctions to get embargoed U.S.-origin technology to Iran and oversaw a cover-up campaign designed to destroy and distort evidence of its criminal wrongdoing. When the ZTE USA general counsel learned of the company-wide scheme, he became a whistleblower that spawned massive criminal investigations, prosecutions, and fines.
- (iii) **Huawei Co.** showed consciousness of guilt because it devised a scheme to conceal its role in sourcing embargoed U.S.-origin goods and services to Iran, while directing its officers, including its CFO, to make multiple material misrepresentations to U.S. authorities and financial institutions to conceal the scope and nature of its Iranian business. Further, when Huawei learned of the U.S. government’s investigations concerning Huawei’s Iranian interests, Huawei Co. ordered its employees, and the employees of its subsidiaries, including Huawei Device USA, to destroy documentary evidence and remove witnesses outside the jurisdiction of the U.S. authorities.

1144. Defendants’ consciousness of guilt can **only** be explained by each Defendants’ knowledge that the IRGC’s “security” assistance needs comprised knowingly providing material support for the terrorist agenda of Hezbollah, the Qods Force, and Regular IRGC for the specific

³⁸⁴ *Canada Stockwatch*, **MKTDIAM Diamonds & Specialty Minerals Summary for Sept. 22, 2014* (Sept. 22, 2014).

purpose of facilitating the anti-American terror “security” operations of Hezbollah, the Qods Force, and Regular IRGC: (a) **inside of Iran**, e.g., joint training camps funded by the IRGC and staffed by Hezbollah, through which the IRGC’s Shiite Terrorist Proxies and Sunni Terrorist Proxies received essential training, safe haven, and logistical support designed to facilitate their terrorist attacks against Americans in Afghanistan, Iraq, Syria, Yemen, Israel, and Europe; and (b) **outside of Iran**, including, but not limited to, through IRGC proxies in Afghanistan, Iraq, Syria, Yemen, Israel, and Europe.

1145. This conclusion is ineluctable for several reasons. With respect to the phrase “defensive, security, and political cooperation,” two of those three items were unquestionably legal in Defendants’ home countries. At all relevant times, South African and Chinese companies could legally sell weapons to Iran, and therefore it is implausible that Defendants were worried about the criminal risk of facilitating weapons sales from South Africa because however disgusting such conduct was, it was not illegal under South African law (and MTN Group did not have any U.S. affiliates).

1146. Moreover, the South African and Chinese governments were both longstanding close allies of Iran based upon their unique historical bonds, and in such context, it is implausible that Defendants were concerned about breaking the law by promoting “political cooperation” between their respective countries and Iran, since “political cooperation” with Iran was a perfectly acceptable thing in both South Africa and China at all relevant times.

1147. **Only** Defendants’ knowledge that “security” meant “Hezbollah, Qods Force, and anti-American terror” explains the totality of each Defendant’s conduct, as well as the parallel nature of their crimes, e.g., rampant document destruction. For Defendants to facilitate a helicopter sale to the regular Iranian Army (not the IRGC), or help broker political cooperation,

was not only legal, but in furtherance of the economic and political agendas of all but the U.S. Manufacturer Defendants' home countries, South Africa and China. For Defendants to agree to provide "security assistance" to the IRGC (including Hezbollah and the Qods Force), however, was a categorically different matter.

1148. With respect to MTN Group and MTN Dubai, directly assisting the "security" operations of Hezbollah, the Qods Force, and Regular IRGC plainly ran the risk of committing a litany of crimes under South African law (e.g., terrorism crimes and espionage), and created obvious – and dire – potential risk to any MTN Group or MTN Dubai executive, employee, or agent who participated in the Conspiracy without making a noisy withdrawal. Indeed, to this date, MTN Group and MTN Dubai have yet to exit the Conspiracy.

1149. With respect to ZTE and Huawei, the motivation to conceal their direct "security" assistance to the IRGC was rooted in an obvious explanation: both sought to facilitate the hostile activities of the Chinese Communist Party that aided the IRGC's Shiite Terrorist Proxies and the IRGC's Sunni Terrorist Proxies in order to facilitate attacks against targeted Americans in Afghanistan, Iraq, and throughout the Middle East to drive the U.S. out so that China could become the dominant regional power consistent with the ideology and agenda of the Chinese Communist Party.

C. Defendants Knew Their Illicit Transfers Of Cell Phones To Hezbollah, The Qods Force, And Regular IRGC Aided the Conspiracy's Terrorist Attacks Against Americans Worldwide

1150. Defendants knew that their illicit provision of U.S. smartphones, computing technologies, and other items requested by Hezbollah, the Qods Force, and Regular IRGC was an act of international terrorism because Defendants knew that such phones, supplied in such volumes to such terrorists, would fund and logistically aid thousands of terrorists every year.

1151. Defendants knew that Hezbollah, the Qods Force, and IRGC proxies like al-Qaeda, depended upon reliable supplies of cell phones as a key growth engine for expanding the shared global terrorist enterprise they needed to effectively counter the U.S. and NATO and kill Americans in Afghanistan and Iraq. For example, as the *Montreal Gazette* reported at the time:

Under [] Ahmadinejad [], U.S. officials said, the [IRGC] has moved increasingly into commercial operations, *earning profits* and extending its influence in Iran in areas involving big government contracts, including ... *providing cell phones*. Washington has claimed the Revolutionary Guard's Quds Force wing is responsible for the growing flow of explosives, roadside bombs, rockets and other arms to Shiite militias in Iraq and the Taliban in Afghanistan. Quds Force has also been blamed for supporting Shiite allies such as Lebanon's Hezbollah and to such Sunni movements as Hamas and the Palestinian Islamic Jihad.³⁸⁵

1152. Defendants knew that, since 9/11, *every* major transnational Islamist terrorist organization that has targeted Americans has prioritized providing its operatives have a robust, reliable, and covert supply of two material items above all else: stockpiling vast quantities of secure, untraceable American mobile phones, and obtaining as much U.S. currency as possible. This maxim holds true for Shiite and Sunni groups alike, including, but not limited to, the IRGC (including Hezbollah and the Qods Force) Jaysh al-Mahdi, al-Qaeda, the Taliban (including its Haqqani Network), ISIS, al-Nusra Front, and every other major group.

1153. Decades of media coverage alerted Defendants to Hezbollah's specific reputation for using cell phones to help commit terrorist violence.³⁸⁶

³⁸⁵ Montreal Gazette (Canada), *What is the Revolutionary Guard?* (Aug. 16, 2007), 2007 WLNR 28659733.

³⁸⁶ See, e.g., Marjorie Miller, *Hezbollah Battles to Shed Extremist Image in Lebanon*, Los Angeles Times (Nov. 28, 1997) ("Hezbollah us[ed] mobile phones to coordinate attacks and roadside bombs camouflaged as rocks."), 1997 WLNR 5640765; Montreal Gazette (Canada), *B.C. Men Accused of Aiding Hezbollah* (Mar. 29, 2001) ("Two men ... were accused of aiding the Islamic extremist group Hezbollah in an indictment ... They are said to have conspired to provide Hezbollah with cash, night-vision goggles, global-positioning devices, mine-detection equipment, cell phones and blasting equipment."), 2001 WLNR 6561271; Carolynne Wheeler,

1154. Indeed, Defendants were alerted by Hezbollah's own public statements taunting the United States concerning a purported "US 'request' for information on mobile phones."³⁸⁷

D. Defendants Knew That Their Protection Payments To The Taliban, Facilitated Terrorist Attacks By Al-Qaeda And The Taliban Against Americans In Afghanistan And Were Opposed By The U.S. Government For That Reason

1. Defendants Knew That Their Cash And "Free Goods" Protection Payments To The Taliban, Financed, Armed, And Logistically Sustained Terrorist Attacks By Al-Qaeda And The Taliban Against Americans In Afghanistan

1155. Defendants knew (or recklessly disregarded) that they were supplying funding to Taliban terrorists intent on attacking Americans in Afghanistan. The Taliban openly proclaimed

Israeli Troops Enter Village in Lebanon, globeandmail.com (Toronto), (July 22, 2006) ("Air strikes took out relay towers belonging to Lebanon's three main cellular phone companies, Hezbollah's al-Manar television network ... Such communications channels are traditional targets ahead of military action."), 2006 WLNR 27225853; Detroit Free Press, *Israeli Push Deepens Conflict* (July 23, 2006) ("Capt. Jacob Dallal, an Israeli army spokesman, said the targets of the strikes were Al-Manar and Al-Nour, Hizballah's TV and radio stations, respectively. He said five of the radio station's antennas were hit. 'It's important to understand why the attack was carried out,' Dallal said. 'This will disrupt their ability to communicate,' he said, adding that cell phones were a 'key communication link' for Hizballah."), 2006 WLNR 25249492; Jonathan Foreman, *Defusing the Iraqi Conflict*, Daily Mail (UK) (Nov. 2, 2007) ("Back at base, [Chris] Hunter [a "veteran 'ammunition technical officer' or counterterrorist bomb-disposal expert"] looks for patterns in the way that bombs are made and laid. At first his main opponent is a Sunni bomb-making gang, who are happy to slaughter scores of Shia civilians along with Coalition soldiers. Then, in the spring of 2004 comes the Shia militia uprising. They increasingly receive high-tech help from Iran and even Lebanese Hezbollah in using devices such as mobile phones to detonate bombs by remote control."), 2007 WLNR 21680052; Kenneth Timmerman, *Fear Grips Democracy in Lebanon*, Washington Times (Mar. 2, 2009) ("Almost everyone I met warned me about using my cell phone. It was common knowledge that Hezbollah officers in the security forces were regularly intercepting phone calls and tracking their human targets by triangulating the signals the phones send out to cell phone towers around the city."), 2009 WLNR 4034008.

³⁸⁷ Al-Sharq al-Awsat, BBC International Reports (Middle East), *Lebanese Hezbollah Reacts to US "Request" For Information on Mobile Phones* (Mar. 3, 2010) ("Lebanese Hezbollah reacts to US "request" for information on mobile phones. Accusations against the US Embassy in Beirut that it seeks to obtain sensitive information on the mobile phone networks raised doubts within Hezbollah. Hezbollah has doubts that this information might be used by the US intelligence in infiltrating the communications network and tracking Lebanese figures.").

that the money was for terrorism: as the Taliban told one subcontractor in a typical example, “You know we need this American money to help us fund our Jihad.”³⁸⁸ The demands for payments, which the Taliban itself tied to the insurgency, alerted Defendants to the connection between the payments and insurgent violence. As one security firm that faced demands for protection money acknowledged in a November 2007 memorandum, it was obvious that “[i]f we make payment that money will be funneled back into [the Taliban’s] fight against the Coalition.”

1156. Defendants also negotiated their payments in circumstances that left no doubt about whom they were financing. With respect to the large-scale payments negotiated directly with the Quetta Shura, Defendants (or their agents) met with high-level Taliban representatives who openly represented the Taliban’s Financial Commission. The payments to local Taliban officials likewise occurred via negotiations with commanders or shadow “governors” who openly identified as Taliban members. Given the Taliban-controlled geographies in which Defendants operated, Defendants assuredly knew (or recklessly disregarded) that the officials they were paying off worked for the Taliban.

1157. The Taliban memorialized its protection racket in documents that further notified Defendants that they were financing terrorists. Most prominently, the Taliban often conveyed its demands for protection payments in so-called “Night Letters.” Night Letters – whose name comes from their frequent delivery during the night – were documents on official Taliban letterhead bearing the Taliban’s insignia. Although Night Letters could convey a variety of threats, the Taliban commonly sent them to companies to demand protection payments. One typical example, delivered to phone companies in Wardak Province, stated that “we are expecting you to provide financial support for the Taliban stationed in Saidabad district. If you

³⁸⁸ *Afghan Firms Pay Off Taliban.*

cannot, then you should stop your work. Otherwise you have no right to complain in the future (we are warning you of future incidents).” Another, authored by the “Islamic [Emirate] of Afghanistan” (the Taliban’s formal name for itself), informed a local construction company that it “cannot continue to work unless it does obtain permission from the Mojahedeen. Or else, it does not have the right to complain.” Night Letters were widespread in Afghanistan, particularly in areas of Taliban control, and were one of the principal means through which the Taliban communicated its demands for protection money to companies, including Defendants.

1158. Similarly, after effecting the payments, companies regularly received so-called “tax receipts” from the Taliban, providing them with documentation proving they had paid their dues to the insurgents. The Taliban Financial Commission encouraged the provision of tax receipts as a way of further standardizing and accounting for the revenue raised through the insurgents’ protection rackets. And those tax receipts – like the Night Letters – appeared on Taliban letterhead and made clear on their face that protection money was intended for the Taliban’s benefit. On information and belief, Defendants or their agents received Night Letters and Taliban tax receipts in connection with their projects in Afghanistan.

1159. Defendants did not believe – nor was it true – that their payments were necessary for them to avoid imminent death or serious bodily injury. The Taliban typically did not extract protection payments by physically confronting companies and threatening immediate violence; rather, the threats were often vaguer and futuristic – as in the Night Letters mentioned above. Many times, those threats were directed at Defendants’ equipment or projects, rather than their personnel. Given the non-immediate nature of the threats, Defendants could notify the U.S. government of the Taliban’s protection racket and try to enlist the military’s assistance in

responding. But rather than avail themselves of such options, Defendants decided that the simplest (and most profitable) option was to make the payments the Taliban demanded.

1160. Defendants' practice of funneling many (though far from all) of their payments through subcontractors, only heightens their culpability. Defendants intentionally used the contracting process to insulate themselves from the payments on paper, but that process – offloading responsibility to local subcontractors several layers removed – was simply their technique for encouraging the payments while avoiding responsibility.³⁸⁹ The payments may often have been physically delivered by an intermediary, but Defendants knew they were occurring and purposefully orchestrated them. That is because Defendants could only obtain their desired business outcome by ensuring that their money actually reached the Taliban. Had Defendants' subcontractors spent the money on some other, legitimate purpose, rather than directing it to the Taliban, Defendants would not have obtained the security benefit they wanted.

1161. Western contractors have confirmed their understanding that, during the relevant timeframe, local intermediaries were routing contract money to the Taliban on their behalf. The head of one private-security company admitted that his “boss wouldn’t appreciate it if I went to negotiate face to face with the tribal leaders of Helmand” – historically a key part of Taliban leadership – so he instead used “intermediaries who recruit our security guards locally.”³⁹⁰ Exemplifying the no-questions-asked mentality typical of many contractors, the executive stated, “You just hope they’re not linked too closely with the Taliban.”³⁹¹

³⁸⁹ As General Petraeus explained in formal contracting guidance designed to further discourage protection payments to the Taliban, “[e]xcessive sub-contracting tiers provide opportunities for criminal networks and insurgents to divert contract money from its intended purpose.” *COMISAF’s Contracting Guidance* at 1 (September 2010).

³⁹⁰ *Taliban’s Secret Weapon*.

³⁹¹ *Id.*

1162. Another contractor negotiating a shipment of pipes through Helmand confirmed to a reporter that he typically “tacked on about 30 percent extra for the Taliban,” which he accounted for as “transportation costs” charged back to the prime contractor running the project.³⁹² When the “foreign contractor in charge of the project” was asked about it, the contractor admitted, “We assume that our people are paying off the Taliban.”³⁹³

1163. Yet another American contractor admitted that his protection payments – amounting to 16% of his gross revenues – were “all revenue that will ultimately be shared by the Taliban.”³⁹⁴ This contractor was well aware of the consequences: “‘All of this could be seen as material support for enemy forces,’ he muse[d]. ‘But you have to weigh that against everything that is being done in that project. Are you aiding and abetting the enemy if you have to pay to get a school built? It’s the cost of doing business here.’”³⁹⁵

1164. By no later than 2008, Chinese media reports specifically alerted Defendants that the Taliban, relied upon communications technologies to conduct attacks against Americans in Afghanistan. For example, on February 25, 2008, *Xinhua News Agency*, which is a Chinese Communist Party analogue to the Associated Press, reported that the “Taliban threaten[ed] Afghan mobile telecom companies,” which alerted Defendants to the Taliban’s communications technology rackets in Afghanistan.³⁹⁶

³⁹² *Funding The Afghan Taliban*.

³⁹³ *Id.*

³⁹⁴ *How The Taliban Thrives* at 50.

³⁹⁵ *Id.*

³⁹⁶ *Xinhua News Agency, Taliban Threatens Afghan Mobile Telecom Companies* (Feb. 25, 2008).

1165. At all relevant times, it was common knowledge among businesses operating in Afghanistan, including Defendants, that Western contracting dollars were flowing to the Taliban in the form of protection money. Because the Taliban openly demanded the money – and because local subcontractors openly paid it – companies on the ground in Afghanistan were widely aware of the practice. One journalist referred to such payments as an “open secret”³⁹⁷; another called protection payments a “widely known practice in Afghanistan”³⁹⁸; and experts described it to *CBS News* as an “open secret on the streets.”³⁹⁹ Defendants were sophisticated companies with millions of dollars in revenues on the line in Afghanistan. They were aware of this prevailing understanding that their “security” payments were flowing to the Taliban.

1166. A *Time Magazine* cover story on September 7, 2009, entitled “Taliban Inc. – How Drugs, Extortion, Protection Rackets And Foreign Aid Fuel The Afghan Insurgency,” accompanied a full-page cover graphic depicting an AK-47 lying on top of a box full of \$100 bills. In the article, the author noted that “protection payments are so widespread that one contractor I interviewed responded incredulously to questions about how the system worked. ‘You must be the only person in Afghanistan who doesn’t know this is going on,’ he said.”⁴⁰⁰

1167. From the mid-2000s onward, accounts from other prominent media sources also reported that multinational corporations, including their contractors and subcontractors, were redirecting Western contract funds to the Taliban. Those widespread reports further informed Defendants that their expenditures in Afghanistan were delivering protection money to the Taliban. Examples of such reports included, but were not limited to:

³⁹⁷ *Funding The Afghan Taliban*.

³⁹⁸ Dana Chivvis, *Is The Taliban Getting A Cut Of U.S. Aid?*, CBS News (Sept. 3, 2009).

³⁹⁹ Nancy Cordes, *Is Taxpayer Money Funding The Taliban?*, CBS News (Sept. 3, 2009).

⁴⁰⁰ *How The Taliban Thrives* at 50.

- (i) *BBC International Reports (Europe)*, October 2004: “[T]he merging of organized crime and terrorism is a new phenomenon. BND President Hanning assumes ‘that terrorist structures, such as **the Taleban and Al-Qa’idah, finance their fight through the extortion of protection money** as well as direct involvement in drug-trafficking.’”⁴⁰¹
- (ii) *National Post*, September 2006: “The Taliban still have a partnership with al-Qaeda, which provides them training and foreign fighters. ...[T]he Taliban **is** also ... **taking protection money like any mafia**, and using that money to fund their insurgency.”⁴⁰²
- (iii) *Times Record News*, August 2008: “The Taliban tried a similar cell phone tower extortion racket, but it backfired. StrategyPage reported on June 15 that **the Taliban were expanding ‘their extortion campaign, demanding that businesses pay “protection money” to avoid being attacked’** and an effort by the Taliban ‘to control cell phone use has quickly evolved into just another extortion campaign.’ . . . ‘But then, noting that there were several cell phone companies operating in southern Afghanistan, **the Taliban went to the different companies and offered not only “protection,” but damage to a competitor, for a price.**’”⁴⁰³
- (iv) *Inter Press Service*, September 2008: “Often ... logistics companies ... pay protection money ... In one route, ...**contractors pay millions in protection money, some of which may end up in the hands of the Taliban**, [Matthew] Leeming says.”⁴⁰⁴
- (v) *Deutsche Presse Agentur*, June 2009: “Afghanistan’s private sector ... finance[s] the insurgency ... **Those who ... do business ... pay protection money to the Taliban.** ‘Everything has to do with money,’ said [Khalid] Naderi, who co-owns a telecommunications firm that operates in the [] south, where he pays \$2,000 in protection money per month for each ... mast[.]. ‘You have to do it. Everybody does.’”⁴⁰⁵
- (vi) *Frankfurter Rundschau* (Germany), July 2009: “**In the cases of major projects**, contractors have to have the construction plans and bidding documents scrutinized by Taleban engineers after which **the amount of the charge is fixed.**”⁴⁰⁶
- (vii) *Time Magazine*, September 2009: “[Sargon] Heinrich says some 16% of his gross revenue goes to ‘facilitation fees,’ mostly to protect shipments of valuable equipment coming from the border. ‘**That is all revenue that will ultimately be shared by the Taliban.**’ . . . In fact, **protection payments are so widespread** that one contractor I

⁴⁰¹ BBC International Reports (Europe), *German Intelligence Chief Says Bin-Ladin Still Alive* (Oct. 10, 2004). All emphases in this paragraph are added.

⁴⁰² Jaap de Hoop Scheffer, *The World Can Do More: NATO’s Secretary-General On What Afghanistan Needs*, *National Post* (Sept. 13, 2006), 2006 WLNR 26238821.

⁴⁰³ *Times Record News*, *Anatomy Of Terror* (Aug. 21, 2008), 2008 WLNR 31329261.

⁴⁰⁴ Anand Gopal, *Afghanistan: Subsidised Fuel Trail Winds Back To Pakistan*, *Inter Press Service* (Sept. 30, 2008).

⁴⁰⁵ *How The Taliban Has Turned Extortion Into A Gold Mine*.

⁴⁰⁶ Willi Germund, *Steuergeld für Taliban*, *Frankfurter Rundschau* (July 1, 2009) (quoted by Thomas Ruttig, *The Other Side* at 20-21, *Afghanistan Analysts Network* (July 2009)).

interviewed responded incredulously to questions about how the system worked. ‘**You must be the only person in Afghanistan who doesn’t know this is going on,**’ he said.”⁴⁰⁷

- (viii) Sydney Morning Herald, September 2009: “The Taliban also keep an eye on local individuals who get work on the project – especially those doing the all-important security jobs. . . . **Deals in which the Taliban top up their coffers by demanding as much as 30 per cent of the value of a contract as protection money are rife.**”⁴⁰⁸
- (ix) Washington Post, March 2010: “According to senior Obama administration officials, **some of [the money] may be going to the Taliban, as part of a protection racket** in which insurgents and local warlords are paid to allow the trucks unimpeded passage, often sending their own vehicles to accompany the convoys through their areas of control. The essential question, said an American executive whose company does significant work in Afghanistan, is ‘**whether you’d rather pay \$1,000’ for Afghans to safely deliver a truck, even if part of the money goes to the insurgents**, or pay 10 times that much for security provided by . . . contractors.”⁴⁰⁹
- (x) New York Times, May 2011: “Critics say that **payoffs to insurgent groups**, either directly or indirectly, **by contractors** working on highways and other large projects in Afghanistan **are routine**. Some **officials say they are widely accepted in the field as a cost of doing business**, especially in areas not fully under the [government] control...”⁴¹⁰
- (xi) Agence France Presse, September 2012: “‘**Revenue extorted from nationwide enterprises** such as . . . construction and trucking companies, mobile telephone operators, . . . and aid and development projects **goes to the Taliban Financial Commission** which answers to the Taliban leadership,’ said the report [by the U.N. al-Qaeda/Taliban sanctions team]. . . . The [U.N.] sanctions experts said the Taliban have made foreign development funds a ‘lucrative source’. ‘**Estimates of Taliban income from contracts funded by . . . overseas donors range from 10 percent to 20 percent** of the total, usually by the Taliban agreeing protection money with the contractor or demanding a cut.’”⁴¹¹
- (xii) The Hindu, September 2012: “[C]ontractors in Afghanistan often **say they have to make payoffs of between 10 and 20 percent to ensure work can go ahead**. In Farah, local officials have claimed that the payoffs are as high as 40 per cent.”⁴¹²

⁴⁰⁷ *How The Taliban Thrives* at 50.

⁴⁰⁸ *Insurgents Play A Perilous Mountain Game*.

⁴⁰⁹ *Afghan Corruption*.

⁴¹⁰ Alissa J. Rubin & James Risen, *Costly Afghanistan Road Project Is Marred By Unsavory Alliances*, N.Y. Times (May 1, 2011) (“*Afghanistan Road Project Marred By Unsavory Alliances*”).

⁴¹¹ Agence France Presse, *Taliban Made \$400mn In 2011 From Taxes, Extortion: UN* (Sept. 11, 2012), <https://www.nation.co.ke/news/world/Taliban-made--400-mn/1068-1504748-w0sl0a/index.html>.

⁴¹² Praveen Swami, *Why Terrorists Aren’t Scared of Sanctions*, The Hindu (Sept. 12, 2012).

1168. On information and belief, Defendants were aware of these reports or similar ones, and their substance, which documented how protection payments made by Western contractors and subcontractors financed the Taliban's terrorist attacks. Defendants are sophisticated companies, all of which specialize in performing work in high-risk countries like Afghanistan. Given their business models, and the contractual role they undertook to monitor the local security environment, Defendants each monitored open-source reporting on the risks of operating in Afghanistan. As part of those efforts, Defendants' standard practice would have been to conduct basic research on the Afghan market and the mechanics of local subcontracting. Even cursory research of that nature would have uncovered the press reports discussing protection payments set forth above, or other similar reports.

1169. Defendants' above-described knowledge applied equally to Defendants' "free goods" payments of cell phones to al-Qaeda and the Taliban. At all times, Defendants knew that al-Qaeda, the Taliban, and their allies prioritized obtaining U.S.-purchased cell phones for such phones' unique operational benefits to the terrorists.

1170. In the decades after 9/11, press reports regularly alerted Defendants to the Syndicate's desire to source U.S.-purchased phones to facilitate attacks against Americans in Afghanistan. On June 20, 2003, for example, the *Boston Globe* reported that al-Qaeda operative "Iyman Faris" "pleaded guilty to providing material support to terrorists and conspiracy to provide support" and admitted that he "attended an Al Qaeda training camp in Afghanistan," and, thereafter, "transported a cache of money and cellular phones for Al Qaeda" in "Afghanistan for use by bin Laden's fighters."⁴¹³ A few months later, the *Associated Press*

⁴¹³ Amber Mobley, *U.S. Citizen Admits Planning Al Qaeda Attack Trains and a Bridge Allegedly on Hit List*, *Boston Globe* (June 20, 2003), 2003 WLNR 3428108; see Derrill Holly, 20 years for alleged bridge plot;

reported that “[p]rosecutors” stated that “Faris” “assisted al-Qaeda’s work” when he “traveled to Pakistan and Afghanistan” and “carr[ie]d out low-level missions for [al-Qaeda] terrorists” by, among other things, “provid[ing]” “cell phones and cash to al-Qaeda members.”⁴¹⁴

1171. In later years, similar media reports documented al-Qaeda’s continuing efforts to source communications technologies, cell phones, and similar dual-use weapons from the United States. For example, on June 7, 2010, it was widely reported that a “federal grand jury” “charged a Texas man with attempting to provide al Qaeda with global positioning instruments, cell phones and a restricted publication on U.S. weapons in Afghanistan.”⁴¹⁵

1172. Such reports also alerted Defendants that al-Qaeda’s and the Taliban’s reliance upon iconic American communications technologies deepened in the late 2000s, not unlike the knowledge, communications security, and communications efficiency benefits, among others, familiar to most smartphone users after the iPhone revolutionized the space in the late 2000s.

2. Defendants Knew That The U.S. Government Opposed Defendants’ Payment Of Protection Money To The Taliban

1173. The U.S. government did not approve, publicly or privately, of Defendants’ protection payments. At all times, the government conveyed the message that protection payments violated U.S. law and undermined U.S. foreign-policy objectives in Afghanistan.

1174. The U.S. government has long been on record that protection payments to terrorists are unlawful – no matter their motivation. On March 19, 2007, Chiquita Brands International, Inc. (“Chiquita”), a multinational banana supplier, pleaded guilty in this District to

⁴¹⁴ Derrill Holly, *20 Years For Alleged Bridge Plot; Iyman Faris, 34, Tried to Withdraw a Guilty Plea; Prosecutors Say He Assisted Al-Qaeda’s Work*, Associated Press, reprinted in Philadelphia Inquirer (October 29, 2003), 2003 WLNR 14764150.

⁴¹⁵ David C. Morrison, *Behind the Lines: Our Take on the Other Media’s Homeland Security Coverage*, CQ Homeland Security (June 7, 2010), 2010 WLNR 11991958.

having provided material support to the United Self-Defense Forces of Colombia (“AUC”) in Colombia.⁴¹⁶ Chiquita had routed protection payments to the AUC – then designated as a Specially Designated Global Terrorist – “through various intermediaries,” and had falsely accounted for them as “security payments.”⁴¹⁷ Chiquita later argued that it paid AUC protection money “under threat of violence,” but the U.S. Department of Justice responded that the “payments were illegal and could not continue.”⁴¹⁸ It thus charged Chiquita with (and Chiquita pleaded to) the federal crime of transacting with a Specially Designated Global Terrorist.⁴¹⁹

1175. In the public press release announcing the plea deal, an Assistant Attorney General stated: “Like any criminal enterprise, a terrorist organization needs a funding stream to support its operations. . . . Thanks to Chiquita’s cooperation and this prosecution, that funding stream is now dry and corporations are on notice that they cannot make protection payments to terrorists.”⁴²⁰ A U.S. Attorney further emphasized: “Funding a terrorist organization can never be treated as a cost of doing business. . . . American businesses must take note that payments to terrorists are of a whole different category. They are crimes.”⁴²¹ Defendants knew of the *Chiquita* settlement and its clear message that the U.S. government considered protection payments illegal. The settlement received extensive scrutiny among the international business

⁴¹⁶ See Plea Agreement, *United States v. Chiquita Brands Int’l, Inc.*, No. 07-cr-00055-RCL (D.D.C. filed Mar. 19, 2007), Dkt. 11.

⁴¹⁷ Press Release, U.S. Dep’t of Justice, *Chiquita Brands International Pleads Guilty To Making Payments To A Designated Terrorist Organization & Agrees To Pay \$25 Million Fine* (Mar. 19, 2007) (“*Chiquita Brands International Pleads Guilty*”).

⁴¹⁸ *Id.*

⁴¹⁹ See 50 U.S.C. §§ 1701, 1705; 31 C.F.R. §§ 594.201(a), 594.701(c); Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 25, 2001).

⁴²⁰ *Chiquita Brands International Pleads Guilty*.

⁴²¹ *Id.*

community and was the subject of recurring media reports. Outlets describing the settlement included *United Press International* on March 14, 2007; the *Washington Times* on March 19, 2007; the *Associated Press* the next day; and the *Washington Post* on August 2, 2007.⁴²²

1176. The U.S. government viewed protection payments in Afghanistan the same way. Government officials stated that, as with Chiquita's payments to terrorists in Colombia, protection payments to the Taliban were unlawful and undermined U.S. reconstruction objectives. For example, at a House Subcommittee hearing, an Assistant Deputy Defense Undersecretary for Program Support was asked whether "facilitation payments . . . to provincial governors, to local police or warlords in order to ensure that trucks aren't bothered [are] legal under United States law?"⁴²³ He responded: "Clearly, it's not . . . and it's counterproductive to what we're trying to do."⁴²⁴ The U.S. Special Inspector General for Afghanistan Reconstruction ("SIGAR") similarly opined that "I don't think that there should ever be or ever condone paying off a Taliban entity for anything . . . Obviously that's wrong; it's against the law and counter to any counterinsurgency or reconstruction initiative that we would like to see put in place."⁴²⁵

1177. The congressional Commission on Wartime Contracting found it "particularly alarming" that "subcontractors on U.S.-funded convoys, road construction, and development

⁴²² See United Press International, *Chiquita To Pay \$25M For Terrorist Payoffs* (Mar. 14, 2007); Matt Apuzzo, *Chiquita Pleads Guilty To Doing Business With Terrorists*, Assoc. Press (Mar. 20, 2007); *Chiquita Pleads To Protection Payoffs*, Wash. Times (Mar. 19, 2007); Carol D. Leonnig, *In Terrorism-Law Case, Chiquita Points to U.S.*, Wash. Post (Aug. 2, 2007).

⁴²³ *Hearing on Corruption in Afghanistan Defense Contracting* (statement by Rep. John F. Tierney (D. Mass.)).

⁴²⁴ *Id.* (statement of Assistant Deputy Undersecretary Gary Motsek).

⁴²⁵ *Funding The Enemy* at 196.

projects pay insurgent groups for protection.”⁴²⁶ Based on such statements, Defendants knew that the U.S. government was institutionally opposed to protection-money payments.

1178. As the U.S. government became aware of broader patterns of protection payments in Afghanistan, it implemented a number of programs to curtail them. The net effect of these various efforts was to elevate anti-corruption to a distinct line of effort in the Coalition’s campaign plan, and to convey unmistakably to industry participants that protection payments were unacceptable. The U.S. government also implemented a broader array of programs designed to combat corruption in Afghanistan. The outgoing ISAF Commander underscored the importance of those measures to U.S. policy: as he briefed President Obama in 2013, “corruption is the existential, strategic threat to Afghanistan.”⁴²⁷ Defendants’ payments fueled the type of corruption that U.S. agencies were attempting to eradicate.

1179. The U.S. government on occasion encouraged companies to hire local Afghans or employ local Afghan businesses in connection with some projects. This was not a license for Defendants to hire Taliban fighters or to allow their Afghan partners to pay insurgents. On the contrary: the U.S. government at all times communicated an expectation that Defendants should vet their local partners and take affirmative steps to ensure that the money they paid to those partners did not flow to the Taliban. And the U.S. government repeatedly made clear that the payment of protection money – or the payment of Taliban “taxes” – in exchange for permission to proceed with U.S.-funded projects was illegal and counterproductive. Neither USAID nor ISAF ever suggested that such payments were either an inevitable consequence or an acceptable cost of implementing U.S.-funded projects in Taliban areas.

⁴²⁶ *CWC Report* at 73.

⁴²⁷ Joint and Coalition Operational Analysis (JCOA), *Operationalizing Counter/Anti-Corruption Study* at 1 (Feb. 28, 2014) (emphasis in original), <https://www.hsdl.org/?view&did=756004>.

IX. DEFENDANTS' FINANCIAL, LOGISTICAL, AND OPERATIONAL AID TO THE IRGC AND PROTECTION PAYMENTS TO THE TALIBAN FLOWED THROUGH TO FACILITATE TERRORIST ATTACKS AGAINST AMERICANS IN AFGHANISTAN THAT WERE PLANNED, AUTHORIZED, AND OFTEN JOINTLY COMMITTED BY AL-QAEDA

A. In Furtherance Of The IRGC Conspiracy, The IRGC Relied Upon Defendants' Resources To Provide Key Assistance To Al-Qaeda And The Taliban, That Facilitated Terrorist Attacks Against Americans In Afghanistan In Order To Drive The United States Out Of Afghanistan In Furtherance Of The IRGC's Conspiracy

1180. Defendants provided the funds, technologies, services, and support necessary for the IRGC to sustain its decades-long, robust support for al-Qaeda and the Taliban, including its Haqqani Network, as they mutually sought, alongside the IRGC, to expel the United States from Afghanistan through a campaign of IRGC-sponsored terrorism in Afghanistan that was committed, planned, and authorized by al-Qaeda.

1181. The IRGC has long provided support – routed through Hezbollah and the Qods Force – for al-Qaeda-led terrorist attacks against American military forces and contractors in Afghanistan and Iraq. For example, Hezbollah, the Qods Force, and Regular IRGC sponsored a substantial training, logistics, travel, and communications campaign, all of which was implemented by the IRGC in Lebanon, Iran, Iraq, and Afghanistan) using IRGC, including Hezbollah and the Qods Force, resources that enabled Hezbollah and the Qods Force to flow resources and training to al-Qaeda and Taliban, including Haqqani Network, terrorists who facilitated attacks against Americans in Afghanistan.

1182. The IRGC intentionally used Hezbollah and the Qods Force to lead every aspect of its support for al-Qaeda and Taliban attacks against Americans in Afghanistan, at least in part, because the IRGC wanted “plausible deniability” of Iranian involvement based upon the Iranian propaganda that Hezbollah is not and was not an Iranian agent. To that end, when MTN, ZTE, and Huawei provided embargoed technology and funds, and any other materials useful for

terrorist tradecraft to their IRGC front counterparties, those items flowed through such IRGC-related parties to Hezbollah and the Qods Force, which, in turn, distributed money, arms, and technology to the IRGC's proxies in Afghanistan, al-Qaeda and the Taliban. In this way, the IRGC maintained influence on the Afghanistan Terror Campaign while simultaneously delegating its planning, commission, and authorization to al-Qaeda and the Haqqani Network, who were two of the IRGC's key allies amongst the Syndicate.

1. The IRGC, Including Its Hezbollah Division And Qods Force, Provided Material Support For Anti-American Terrorism In Afghanistan To Undermine The U.S. Mission There

1183. Although there are religious differences between the Shiite Iranian regime and the Sunni Taliban organization, those differences have not deterred the IRGC from supporting the Taliban's terrorist activities. *See, e.g., Cabrera*, at *10-11. The IRGC and the Taliban share a core geopolitical aim: to inflict mass casualties on Americans in the region. As two military intelligence scholars observed, "the Iranian regime is ideologically and religiously opposed to the Taliban, [but] it nevertheless views the group as a useful counterweight to the United States."⁴²⁸ Similarly, as a Taliban commander stated in 2010 of Iran, "Our religions and our histories are different, but our target is the same – we both want to kill Americans." Sectarian distinctions aside, the IRGC has supported and funded attacks by the Taliban on U.S. and allied forces in Afghanistan to harm the United States.

1184. The Fourth Corps of the Qods Force, one of its four regional commands, implements Iran's foreign policy in Afghanistan. During the relevant timeframe, the Qods Force did so largely by providing the Taliban (including the Haqqani Network) with material support for terrorist attacks in Afghanistan. The Fourth Corps' al-Ansar Command Center is based in

⁴²⁸ *Iran's Balancing Act* at 5.

Iran's second-largest city, Mashhad, near the border with Afghanistan. Mashhad naturally serves as a stopping point between Afghanistan and Tehran, Iran's capital.

1185. In the months after 9/11, the IRGC met with senior Taliban officials to offer military aid to support the Taliban's fight against U.S.-led Coalition forces. The IRGC planned that meeting and hosted it on the Iranian side of the Afghanistan border. As part of this initial offer of support, the IRGC pledged to sell advanced military equipment to the Taliban for use against U.S. and allied forces, boasted of the IRGC's ability to track U.S. troop movements, and promised to allow terrorists entering Afghanistan to travel through Iranian territory. The IRGC also provided safe harbor to Taliban leaders who escaped U.S. forces.

1186. Immediately following the U.S. invasion of Afghanistan, the IRGC made a pretense of professing support for the U.S. and NATO mission, but in reality was already seeking to undermine it. On February 6, 2002, then-CIA Director George J. Tenet testified before Congress that "initial signs of Tehran's cooperation and common cause with us in Afghanistan are being eclipsed by Iranian efforts to undermine US influence there. While Iran's officials express a shared interest in a stable government in Afghanistan, the IRGC appeared bent on countering the US presence." As one scholar explained, the IRGC "feared the US might use Afghanistan as a base from which to launch a kinetic attack on Iran. The Taliban insurgency thus became viewed by Tehran as a tool with which to keep American forces preoccupied."⁴²⁹

1187. The U.S. government documented the IRGC's escalating support for the Taliban terrorists over the course of the United States' involvement in Afghanistan. In April 2007, General Peter Pace, Chairman of the U.S. Joint Chiefs of Staff, stated that Iranian explosives had

⁴²⁹ Farhad Rezaei, *Iran and the Taliban: A Tactical Alliance?*, The Begin-Sadat Center for Strategic Studies (Jan. 15, 2019) ("*Iran and the Taliban: A Tactical Alliance?*").

been captured in Kandahar Province en route to the Taliban but acknowledged that it was not yet entirely clear who within Iran was responsible. The next day, U.S. Assistant Secretary of State Richard Boucher described “a series of indicators that Iran is maybe getting more involved in an unhealthy way in Afghanistan.”

1188. Those indicators rapidly grew in intensity, and soon there was little doubt that the IRGC was actively sponsoring the Taliban terrorists as a core part of its foreign policy. A purported May 2007 U.S. State Department cable (as published online), for example, reported that Afghan President Hamid Karzai had expressed concerns “over Iranian agents engaging Taliban and supplying them with weapons.” A purported July 2007 U.S. State Department cable (as published online) similarly reported that Taliban terrorists had received “light weapons and grenade launchers [that] bore the stamps of the Iranian factories where they were manufactured, primarily in 2006 and 2007.” The same cable explained that the fighters claimed they had received training in Iran and had been promised access to antiaircraft rockets by IRGC officials. A purported military intelligence summary the next month (as published online), reported on an “‘alarmingly rapid increase’ in Iranian presence in Afghanistan.”

1189. When the U.S. Treasury Department designated the Qods Force as a SDGT later in 2007, it confirmed that the “Qods Force provides weapons and financial support to the Taliban to support anti-U.S. and anti-Coalition activity in Afghanistan.” Press Release, *U.S. Treasury Dep’t, Fact Sheet: Designation of Iranian Entities and Individuals for Proliferation Activities and Support for Terrorism* (Oct. 25, 2007). As the designation explained:

The Qods Force is the Iranian regime’s primary instrument for providing lethal support to the Taliban. The Qods Force provides weapons and financial support to the Taliban to support anti-U.S. and anti-Coalition activity in Afghanistan. Since at least 2006, Iran has arranged frequent shipments of small arms and associated ammunition, rocket propelled grenades, mortar rounds, 107mm rockets, plastic explosives, and probably man-portable

defense systems to the Taliban. . . . Through Qods Force material support to the Taliban, we believe Iran is seeking to inflict casualties on U.S. and NATO forces. (*Id.*)

1190. Similar observations continued in 2008. According to the U.S. State Department's 2008 Country Reports on Terrorism: "The Qods Force, an elite branch of the Islamic Revolutionary Guard Corps (IRGC), is the regime's primary mechanism for cultivating and supporting terrorists abroad. The Qods Force provided aid in the form of weapons, training, and funding to HAMAS and other Palestinian terrorist groups, Lebanese Hizballah, Iraq-based militants, and Taliban fighters in Afghanistan."

1191. In 2009, the U.S. government's Joint IED Defeat Organization ("JIEDDO") reported that "Iran's intentions are the same in both Afghanistan and Iraq: to develop, fund and arm proxy networks to leverage against the perceived U.S. aim of pursuing an active regime change doctrine in Iran."⁴³⁰

1192. By April 2010, the U.S. Department of Defense publicly reported that the IRGC was "covertly" supporting the Taliban. "Arms caches have been recently uncovered with large amounts of Iranian manufactured weapons, to include 107mm rockets, which we assess IRGC-QF delivered to Afghan militants." DOD further explained that "Tehran's support to the Taliban is inconsistent with their historic enmity, but fits with Iran's strategy of backing many groups to ensure that it will have a positive relationship with the eventual leaders."

⁴³⁰ Similarly, a purported January 2010 cable (as published online) explained that senior officials from the U.A.E.'s State Security Department had accused Iran, through the IRGC, of supporting the Taliban by providing money and weapons, smuggling drugs, and facilitating the movement of Taliban leaders and fighters. According to another purported February 2010 cable (as published by online), President Karzai's Chief of Staff and former Ambassador to Iran reported that Iranian officials were no longer denying the IRGC's support for the Taliban in Afghanistan, instead remaining silent in the face of the assertion by the Government of Afghanistan.

1193. On August 3, 2010, the U.S. Treasury Department – pursuant to Executive Order 13224 – designated General Hossein Musavi and Colonel Hasan Mortezaei, senior officials in the Qods Force, as SDGTs for their roles in supporting the Taliban. Press Release, *U.S. Treasury Dep’t, Fact Sheet: U.S. Treasury Department Targets Iran’s Support for Terrorism Treasury Announces New Sanctions Against Iran’s Islamic Revolutionary Guard Corps-Qods Force Leadership* (Aug. 3, 2010). General Musavi was the leader of the Ansar Corps, also known as the Fourth Corps, the branch of the Qods Force responsible for carrying out activities within Afghanistan. *Id.* The U.S. Treasury Department found that both General Musavi and Colonel Mortezaei, acting in their capacity as senior Qods Force officers, had provided “financial and material support to the Taliban.” *Id.* Treasury further concluded that “the IRGC-QF provides select members of the Taliban with weapons, funding, logistics and training.” *Id.*

1194. General David Petraeus, then the Commander of the ISAF, testified before the Senate Armed Services Committee on March 15, 2011 that the IRGC “without question” supplied weapons, training, and funding to the Taliban in order to “make life difficult” for U.S. and NATO forces in Afghanistan.

1195. When the U.S. Department of Defense provided Congress with its Annual Report on Military Power of Iran in April 2012, it explained that, even though Iranian “support to the Taliban is inconsistent with their historic enmity, it complements Iran’s strategy of backing many groups to maximize its influence while also undermining U.S. and [NATO] objectives by fomenting violence.” By means of “the IRGC-QF, Iran provides material support to terrorist or militant groups such as . . . the Taliban.” The U.S. Department of Defense characterized the support as part of a “grand strategy” to “challeng[e] U.S. influence.”

1196. In its 2012 Report on Progress Toward Security and Stability in Afghanistan, the U.S. Department of Defense reported to Congress that the IRGC was engaging in “covert activities” in Afghanistan, including the provision of weapons and training to the Taliban. As the report explained, “Since 2007, Coalition and Afghan forces have interdicted several shipments of Iranian weapons. Tehran’s relationship with the insurgency, although not ideologically based, is consistent with Iran’s short- to mid-term goal of undermining Coalition efforts and opposing the international military presence in Afghanistan.”

1197. Less than two years later, the U.S. Treasury Department concluded that the Qods Force “utilized now-detained Afghan associate, Sayyed Kamal Musavi, who was designated today, to plan and execute attacks in Afghanistan” and further confirmed that “[t]wo IRGC-QF officers also designated today, Alireza Hemmati and Akbar Seyed Alhosseini, provided logistical support to this associate.” Press Release, *U.S. Treasury Dep’t, Treasury Targets Networks Linked To Iran* (Feb. 6, 2014). Similarly, according to a Taliban commander in central Afghanistan in 2015: “Iran supplies us with whatever we need.”⁴³¹

1198. In 2016, Taliban leader Mullah Mansour was killed by an American drone strike while returning to Afghanistan from Tehran, where he had been meeting with Iranian security officials, and possibly directly with Ayatollah Ali Khameni, to discuss tactical coordination of Taliban terrorist activities in Afghanistan. He had made at least two visits to Iran since 2013.

1199. The IRGC’s support for terrorist groups in Afghanistan has continued. The U.S. State Department stated in June 2017 that “Iran is responsible for intensifying multiple conflicts and undermining the legitimate governments of, and U.S. interests in, Afghanistan” The U.S. Department of Defense similarly stated in June 2017 that the IRGC “provides some support

⁴³¹ Margherita Stancati, *Iran Backs Taliban With Cash And Arms*, Wall St. J. (June 11, 2015).

to the Taliban and Haqqani Network.” In May 2018, U.S. Secretary of State Michael Pompeo publicly accused the IRGC of supporting the Taliban and other terrorist groups in Afghanistan.

1200. In October 2018, the U.S. Treasury Department, pursuant to Executive Order 13224, designated additional Qods Force officials “for acting for or on behalf of IRGC-QF and for assisting in, sponsoring, or providing financial, material, or technological support for, or financial or other services to or in support of, the Taliban.” Press Release, *U.S. Treasury Dep’t, Treasury and the Terrorist Financing Targeting Center Partners Sanction Taliban Facilitators and their Iranian Supporters* (Oct. 23, 2018). The U.S. Treasury Department acted along with the six other member nations of the Terrorist Financing Targeting Center – a multinational, cooperative effort to combat terrorism in the Middle East.

1201. In January 2019, the Secretary of Iran’s Supreme National Security Council, Ali Shamkhani, publicly acknowledged the IRGC’s support for the Taliban, claiming that it was designed to “curb the security problems in Afghanistan.”

1202. Most recently, the United States has recognized the IRGC’s support of the Taliban in the aftermath of Qassem Soleimani’s death. In a press conference in the days after the killing of General Soleimani, Secretary of State Michael Pompeo publicly accused the IRGC of backing the Taliban and associated groups, including the Haqqani Network.

1203. The IRGC, in turn, signaled its continued focus on destabilizing U.S. forces in Afghanistan by appointing General Esmail Ghaani (“Ghaani” or “Qaani”), the former head of the IRGC’s Qods Force branch in Afghanistan, to be the top commander of the Qods Force. General Ghaani traveled to Afghanistan in 2018 as the deputy ambassador of Iran to Kabul and remains focused on cultivating the IRGC’s relationship with the Taliban in Afghanistan.

1204. The Taliban’s reaction to Soleimani’s death similarly recognized the IRGC’s support for its terrorist activities. A Taliban statement condemned American forces for the attack on Soleimani and expressed regret for his “martyrdom.” Additional details were reported in Taliban-aligned publications about Soleimani’s support for the Taliban, including his meeting with Taliban delegations in Iran, personally traveling to Afghanistan, and planning attacks.

1205. Consistent with the policy described above, the IRGC provided material support or resources for the acts of terrorism that killed or injured Plaintiffs or their family members. As explained below, that support took the form of “currency . . . lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, . . . and transportation.”⁴³²

2. The IRGC, Including Its Hezbollah Division And Qods Force, Provided The Taliban, With Weapons, Explosives, And Lethal Substances

1206. The IRGC provided material support or resources for the acts of terrorism that killed or injured Plaintiffs, or their family members, by providing (among other things) weapons, explosives, and lethal substances to the Taliban. Many of the weapons the IRGC provided were designed to be particularly effective against U.S. and allied forces operating in Afghanistan. For example, the IRGC provided the Taliban with anti-tank mines, long range rockets, explosively formed penetrators, suicide vehicle-borne improvised explosive devices, rocket-propelled grenades, and explosives, which were uniquely suited for terrorist attacks on U.S. forces.

1207. From at least 2005 through 2022, the IRGC “provided a range of weapons to the Syndicate including small arms (e.g., AK-47s and other assault rifles), anti-tank missiles, rocket-propelled grenades, surface-to-air missiles, improvised explosive devices (‘IEDs’), explosively

⁴³² 18 U.S.C. § 2339A(b)(1).

formed penetrators (‘EFPs’), rockets, mortars, indirect fire weapons, recoilless rifles, PKM machine guns, ammunition, and components for suicide attacks (e.g., triggers and detonators).” *Cabrera* at *11. Each such weapon-type provided by the IRGC was best-in-class and all were designed for the specific purpose of attacking U.S. forces. The Taliban and its Syndicate allies in Afghanistan used the IRGC’s weapons to kill or injure Plaintiffs or their family members.

3. The IRGC, Including Its Hezbollah Division And Qods Force, Provided The Taliban With Lodging, Training, Expert Advice Or Assistance, Safehouses, Personnel, And Transportation

1208. The IRGC provided material support or resources for the acts of terrorism that killed or injured Plaintiffs, or their family members, by providing lodging, training, expert advice or assistance, safe harbor, and transportation to the Taliban.

1209. Indeed, U.S government officials openly accused the IRGC of training the Taliban. In an August 2009 report, ISAF Commander General Stanley McChrystal publicly explained that “the Iranian Qods Force is reportedly training fighters for certain Taliban groups and providing other forms of military assistance to insurgents.”⁴³³ In August 2010, the State Department publicly reported to Congress: “Iran’s Qods Force provided training to the Taliban in Afghanistan on small unit tactics, small arms, explosives, and indirect fire weapons”⁴³⁴

1210. From at least 2005 through 2022, the IRGC provided the Taliban, including the Haqqani Network, lodging, training, expert advice or assistance, safe harbor, and transportation. *E.g., Cabrera* at *11. The IRGC taught the Taliban attack techniques that were particularly effective against U.S. forces. Without the IRGC’s training, the Taliban would not have been

⁴³³ GEN McChrystal confirmed again in May 2010 that the IRGC was training Afghan fighters in Iran. *Killing Americans and Their Allies*, *supra*.

⁴³⁴ In May 2013, State publicly reported: “the IRGC-QF trained Taliban elements on small unit tactics, small arms, explosives, and indirect fire weapons, such as mortars, artillery, and rockets.”

able to launch as successful a terrorist campaign against U.S. forces. The IRGC's training of Taliban terrorists in small unit tactics, small arms, explosives, indirect fire, and other techniques enabled the Taliban to better attack U.S. forces. The Taliban and its Syndicate allies in Afghanistan used the IRGC's training to kill or injure Plaintiffs or their family members.

1211. Hezbollah and Qods Force terrorists also conducted attacks alongside Taliban terrorists. In an October 2016 Taliban attack in Farah Province, four senior Qods Force agents were killed while aiding the Taliban during the attack, and many of the other Taliban dead were taken across the border to Iran for burial.

4. The IRGC, Including Its Hezbollah Division And Qods Force, Provided The Taliban With Financial Support

1212. The IRGC provided material support or resources for the acts of terrorism that killed or injured Plaintiffs, or their family members, by providing financial support to the Taliban. *E.g., Cabrera* at *12.

1213. The IRGC provided large annual cash payments to the Taliban.⁴³⁵

1214. The IRGC also directly paid Taliban insurgents to kill U.S. forces.⁴³⁶ The IRGC paid Taliban terrorists an estimated \$1,000 for each U.S. soldier murdered in Afghanistan and \$6,000 for each destroyed American military vehicle.⁴³⁷

⁴³⁵ For example, a purported February 2005 military intelligence summary (as published online) reported that the IRGC delivered 10 million Afghanis (worth roughly \$212,000) to a location on Iran's border where the money was transferred to four members of a Taliban-associated group.

⁴³⁶ Another purported February 2005 military intelligence summary (as published online) reported on a Taliban group that was being paid by the Iranian government \$1,740 for each Afghanistan soldier killed and \$3,481 for each Government of Afghanistan official killed. The report further explained that the group would begin attacking U.S. forces if the attacks on Afghans were successful.

⁴³⁷ *E.g., Miles Amoores, Iran Pays the Taliban to Kill US Soldiers*, The Times (Sept. 5, 2010). In one specific example, Taliban fighters received \$18,000 from the IRGC as a reward for an attack in 2010 that killed several Afghan forces and destroyed an American armored vehicle. *Id.*

1215. The IRGC also provided funding to individual Taliban commanders, often as they were returning to Afghanistan from training in Iran.⁴³⁸

1216. The IRGC also supported the Taliban's finances by supporting its ability to traffic narcotics, which Taliban terrorists used "to finance their acts of terror and violence."⁴³⁹

1217. The Taliban and its Syndicate allies in Afghanistan used the IRGC's financial support to fund the terrorist campaign that killed or injured Plaintiffs or their family members.

5. The IRGC, Including Its Hezbollah Division And Qods Force, Provided Material Support to Al-Qaeda to Facilitate Syndicate Attacks in Afghanistan

1218. The IRGC has supported al-Qaeda's terrorist activities since the early 1990s, when bin Laden lived in Sudan. The IRGC, Hezbollah, and Qods Force served as the original trainer for al-Qaeda with respect to suicide bombings, attacks against large buildings, IEDs, explosives, intelligence, and general attack tactics directed at American interests. For example, senior al-Qaeda operatives traveled to Iran and Lebanon during this period to Hezbollah camps sponsored by the Qods Force. *Owens v. Republic of Sudan*, 826 F. Supp. 2d 128, 151 (D.D.C. 2011) ("Prior to al Qaeda members' training in Iran and Lebanon, al Qaeda had not carried out

⁴³⁸ *E.g.*, a purported May 2008 military intelligence summary (as published online) reported on a Taliban leader returning from training in Iran "along with a considerable amount of money." A purported May 2009 U.S. State Department Cable (as published online) stated that the IRGC may provide Taliban Commander Mullah Sangin with financial support to engage Coalition forces, including U.S. contractors.

⁴³⁹ Press Release, U.S. Treasury Dep't, *Treasury Targets Taliban Shadow Governor of Helmand Afghanistan as Narcotics Trafficker* (Nov. 15, 2012). As the U.S. Treasury Department explained when it designated Iranian Qods Force General Gholamreza Baghbani as a Specially Designated Narcotics Trafficker in March 2012, General Baghbani allowed Afghan narcotics traffickers to smuggle opiates through the IRGC, facilitated the smuggling of chemicals necessary to produce heroin from Iran into Afghanistan, and helped "facilitate shipments of opium into Iran." Press Release, U.S. Treasury Dep't, *Treasury Designates Iranian Qods Force General Overseeing Afghan Heroin Trafficking Through Iran* (Mar. 7, 2012). General Baghbani also had narcotics traffickers deliver weapons on his behalf to the Taliban. *Id.*

any successful large scale bombings.”). The operatives received advanced explosives training that enabled al-Qaeda to launch large-scale terrorist attacks on American embassies in Africa. *Id.* According to one senior al-Qaeda official, trainers at this time were already researching how to develop shaped charges to pierce armor plating – the technology later perfected in EFPs.

1219. After 9/11, senior al-Qaeda leadership, sheltering in Iran under the patronage and with the counsel of Qods Force operatives, explicitly modeled their post-9/11 organization and tactics on the approach of Hezbollah and the Qods Force.

1220. While al-Qaeda was re-building itself in Iran after 9/11, the Iranians were busy rejecting U.S. and allied requests to stop aiding al-Qaeda. For example, on or about 2002 or 2003, Iran rejected a lawfully issued extradition request by the Jordanian government for Zarqawi on the preposterous grounds that Zarqawi – whom the Iranians knew well – was not Jordanian but, rather, Syrian. Similarly, in a 2003 face-to-face meeting in Geneva, Switzerland, then-U.S. ambassador to Iraq Ryan Crocker implored Iranian officials to cease their support for al-Qaeda’s terrorism targeting Americans in the Persian Gulf, which request the Iranians refused. By then, al-Qaeda had demonstrated its utility to the IRGC with respect to its ability to kill Americans, and the IRGC was already sheltering and supporting al-Qaeda’s military leader, Saif al-Adel (who was also al-Qaeda’s manager for Zarqawi’s Iraqi activities) in his Qods Force-provided Tehran safehouse.

1221. The Iranians rebuffed U.S. outreach because the IRGC had already reached a secret deal with al-Qaeda. Following the 9/11 attacks on the United States and subsequent routing of Sunni terrorists in Afghanistan (including al-Qaeda) in late 2001, the IRGC met with senior al-Qaeda leaders who had fled Afghanistan into Iran to offer military aid to support al-Qaeda’s fight against America. The IRGC hosted these meetings for its al-Qaeda “guests” throughout 2001 and 2002. As part of this initial offer of support, the IRGC pledged to provide funds and logistical

support to facilitate the development of terrorist activities targeting Americans in countries bordering Iran. While the focus at the time was on Afghanistan, all involved expected the U.S. to eventually move into Iraq and for their shared terrorist enterprise to follow us there.

1222. Under this secret deal between the IRGC and al-Qaeda after 9/11, the IRGC intensified its material support for al-Qaeda's terrorist campaign against Americans around the world. Through the secret deal between the IRGC and al-Qaeda and the assistance that the former provided to the latter thereafter, the IRGC was the proximate and but-for cause of al-Qaeda's survival as a terrorist organization after 9/11 and the al-Qaeda linked terrorist attacks against Americans in Afghanistan, including Plaintiffs, that inevitably followed.

1223. Osama bin Laden personally concluded that al-Qaeda would have collapsed after 2001 without the secret deal and the IRGC's key support for al-Qaeda, and al-Qaeda's subsequent ability to execute terrorist attacks depended upon the "artery" provided by the IRGC. For example, in 2007, bin Laden criticized an al-Qaeda terrorist who had been planning to strike IRGC-linked targets; in a secret internal al-Qaeda communique authored by bin Laden himself, bin Laden identified the key, organization-saving assistance that the IRGC had been providing to al-Qaeda after 9/11, stating because of the IRGC's historical support for al-Qaeda's terrorist operations, Iran was al-Qaeda's "*main artery for funds, personnel, and communication.*"

1224. Zawahiri also emphasized close cooperation between al-Qaeda and the IRGC, following a pragmatic approach under which al-Qaeda focused on expanding its presence in Iran. Like bin Laden, Zawahiri agreed that al-Qaeda could not survive and thrive without the IRGC's support. In a letter reportedly written by Zawahiri, al-Qaeda thanked the IRGC for the Qods Force's support in setting up al-Qaeda's terrorist network in Yemen in 2008 and stated, in effect, that al-Qaeda could not have established its franchise in Yemen without the IRGC's assistance.

1225. The U.S. government has also recognized the close partnership between the IRGC and al-Qaeda after the secret deal between the two. In July 2011, the U.S. Treasury Department designated as SDGTs six members of al-Qaeda operating in Iran under the previously described secret agreement between the IRGC and al-Qaeda.⁴⁴⁰ In so doing, the Treasury Department concluded that the secret deal provided that al-Qaeda terrorists “must refrain from conducting any operations within Iranian territory and recruiting operatives inside Iran while keeping Iranian authorities informed of their activities. In return, the Government of Iran gave the Iran-based al-Qa’ida network freedom of operation and uninhibited ability to travel for extremists and their families” and permitted al-Qaeda to use Iran as a “critical transit point for funding to support [al-Qaeda’s] activities.” The Treasury Department also found that “Iran’s secret deal with al-Qa’ida” facilitated a terrorist network that “serves as the core pipeline through which al-Qa’ida moves money, facilitators and operatives from across the Middle East to South Asia.”⁴⁴¹ Indeed, al-Qaeda honored its commitment to the IRGC despite attacking Shiite Muslims elsewhere in the region.

1226. The U.S. Treasury Department has repeatedly recognized the link between al-Qaeda and the IRGC in making SDGT designations under Executive Order 13224. In February 2012, the agency designated the Iranian Ministry of Intelligence and Security (“MOIS”) as a terrorist-sponsoring entity for, among other things, supporting al-Qaeda.⁴⁴² In 2014, the agency likewise designated a “key Iran-based” al-Qaeda facilitator who has “assisted extremists and operatives transiting Iran on their way into and out of Pakistan and Afghanistan.”⁴⁴³

⁴⁴⁰ Press Release, U.S. Treasury Dep’t, *Treasury Targets Al-Qa’ida Funding and Support Network Using Iran as a Critical Transit Point* (July 28, 2011).

⁴⁴¹ *Id.*

⁴⁴² Press Release, U.S. Treasury Dep’t, *Treasury Designates Iranian Ministry of Intelligence and Security for Human Rights Abuses and Support for Terrorism* (Feb. 16, 2012).

⁴⁴³ Press Release, U.S. Treasury Dep’t, *Treasury Targets Networks Linked To Iran* (Feb. 6, 2014).

1227. The close relationship between al-Qaeda and the IRGC has continued in recent years. In July 2017, the State Department reported, “Since at least 2009, Iran has allowed [al-Qaeda] facilitators to operate a core facilitation pipeline through the country, enabling [al-Qaeda] to move funds and fighters to South Asia and Syria.” State further accused the IRGC of remaining unwilling to bring to justice or identify al-Qaeda members in its custody. The next year, State reaffirmed those conclusions and reiterated the IRGC’s close relationship with al-Qaeda.

1228. The IRGC also supported al-Qaeda through its proxy, Hezbollah. As the *Washington Post* reported at the time in 2002, the IRGC’s lead terrorist proxy, Hezbollah, was “increasingly teaming up with al Qaeda on logistics and training for terrorist operations, according to U.S. and European intelligence officials and terrorism experts.” Dana Priest and Douglas Farah, *Terror Alliance Has U.S. Worried; Hezbollah, Al Qaeda Seen Joining Forces*, Wash. Post (June 30, 2002). “The new cooperation ... includes coordination on explosives and tactics training, money laundering, weapons smuggling and acquiring forged documents, according to knowledgeable sources. This new alliance, even if informal, has greatly concerned U.S. officials in Washington and intelligence operatives abroad who believe the assets and organization of Hezbollah’s formidable militant wing will enable a hobbled al Qaeda network to increase its ability to launch attacks against American targets.” *Id.*

1229. The “collaboration” between the IRGC (through Hezbollah) and al-Qaeda “illustrate[d] what analysts [said] [was] an evolving pattern of decentralized alliances between terrorist groups and cells that share[d] enough of the same goals to find common ground: crippling the United States, and forcing the U.S. military out of the Middle East and Israel out of Palestinian territory. ‘There’s a convergence of objectives,’ said Steven Simon, a former National Security Council terrorism expert.” *Id.* As the *Washington Post* reported, “[a]lthough cooperation between

al Qaeda and Hezbollah may have been going on at some level for years, the U.S. war against al Qaeda [] hastened and deepened the relationship. U.S. officials believe that after al Qaeda was driven from Afghanistan, leader Osama bin Laden sanctioned his operatives to ally themselves with helpful Islamic-based groups, said a senior administration official with access to daily intelligence reports.” *Id.* The *Post* concluded:

European and U.S. intelligence operatives on the ground in Africa and Asia said they have been trying to convince headquarters of the new alliances but have been rebuffed. “We have been screaming at them for more than a year now, and more since September 11th, that these guys all work together,” an overseas operative said. “What we keep hearing back is that it can’t be because al Qaeda doesn’t work that way. *That is [expletive]*. Here, on the ground, these guys all work together as long as they are Muslims. There is no other division that matters.” (*Id.*)

1230. Al-Qaeda’s alliance with Hezbollah continued at all times and proved the intelligence operatives on the ground were right. In June 2012, the Council on Foreign Relations reported that “al-Qaeda ha[d] stepped up its cooperation on logistics and training with Hezbollah, a radical, Iran-backed Lebanese militia drawn from the minority Shiite strain of Islam.”

1231. On or about August 7, 2020, on the anniversary of the IRGC/al-Qaeda bomb attack against U.S. embassies in Africa, Israeli commandos acting at the request of the United States killed al-Qaeda’s number 2 leader, Abu Muhammad al-Masri, in a covert mission in Tehran. Masri was in Iran as a guest of the Iranian government and was permitted to freely plan attacks against the United States from an IRGC-provided safe haven in Tehran. The timing of the attack was not a coincidence, but a rather a professional slap in the terrorists’ face extended by the U.S. and Israeli governments to the IRGC and al-Qaeda, as the latter allies suffered an embarrassing and catastrophic loss on the anniversary of one of their greatest terrorist triumphs.

1232. The mafia-style “Syndicate” of which both the Taliban and al-Qaeda formed a part made attacks by each group more lethal. The IRGC’s mutually reinforcing support for both the Taliban and al-Qaeda made both organizations more effective.

1233. By supporting al-Qaeda and the Taliban, the IRGC provided material support and resources for the attacks that killed or injured Plaintiffs or members of their families. Al-Qaeda and the Taliban directly participated in the attacks that killed or injured Plaintiffs or their family members, which were planned and authorized by al-Qaeda. Moreover, the IRGC was closely intertwined with al-Qaeda and the Taliban and associated terrorist groups acting in Afghanistan, and the IRGC provided weapons, funding, training, cell phones, and logistical support al-Qaeda and the Taliban. Material support and resources provided to the IRGC thus also flowed to al-Qaeda and the Taliban, causing the injury and deaths of Plaintiffs or their family members.

B. In Furtherance Of The IRGC Conspiracy, Al-Qaeda Authorized And Planned The Attacks That Injured Plaintiffs

1234. Since at least the mid-2000s, al-Qaeda authorized and planned the Taliban’s attacks on U.S. forces in Afghanistan in several ways.

1. Al-Qaeda Authorized the Attacks that Injured Plaintiffs

1235. Al-Qaeda provided critical religious authorization for Taliban attacks on U.S. forces. As noted above, in 1998 bin Laden himself directed all Muslims to kill Americans at every opportunity. In the ensuing years, senior al-Qaeda leaders issued a series of *fatwas* directed toward the Taliban, conferring religious permission for them to attack Americans in Afghanistan.

1236. After bin Laden was killed in May 2011, about three months prior to the first attack on a Plaintiff, the Taliban confirmed bin Laden’s religious and moral authority over their Afghan jihad, stating: “Osama Bin Laden You were the *sheikh of the Umma*, a zealous man, and *the scholar and imam of the nation at the level of Jihad* and the fighting of the enemies and

their minions. You were *our* sheikh, *our* imam and *role model*, the *hero and miracle of our times, unique* among your peers, *pious and highly sensible*.”

1237. Consistent with all these activities, al-Qaeda operatives often assumed a position of moral, religious, and tactical authority over Taliban members, often acting “as instructors and religious teachers for Taliban personnel and their family members.”⁴⁴⁴

1238. Al-Qaeda also authorized the Taliban’s terrorist attacks through its participation in Syndicate, which involved periodic mafia-style meetings in which al-Qaeda, the Taliban, and other members of the Syndicate (such as Lashkar-e-Taiba) would confer about geographies and targets to attack.⁴⁴⁵ The Syndicate jointly authorized particular types of terrorist attacks in particular geographies to be carried out by the Syndicate’s individual members. Among other things, the Syndicate specifically approved: (1) the creation and operation of the Kabul Attack Network to attack Americans in Kabul and the surrounding provinces; (2) the campaign of suicide attacks against Americans throughout Afghanistan; (3) the Taliban’s campaign of using anti-American IED and suicide attacks specifically in Nangarhar, Nuristan, Kunar and Laghman (“N2KL”) Provinces and P2K; (4) the Taliban’s “surge” in Kandahar and Helmand from 2010 through 2012; and (5) the Syndicate’s use of, and later aggressive focus on, CAN fertilizer bomb attacks specifically targeting Americans.

1239. Al-Qaeda’s messages of authorization were particularly influential with respect to suicide bombings. In February 2003, bin Laden issued a recording calling specifically for suicide attacks in Afghanistan and Iraq. A few months later, he reiterated in a *fatwa* directed at Afghans that “jihad against [the Coalition] is your duty” and that, “If you start suicide attacks, you will

⁴⁴⁴ Thomas Joscelyn, *Al Qaeda Growing Stronger Under Taliban’s Umbrella, UN Finds*, Long War J. (June 23, 2019) (“*Al Qaeda Growing Stronger*”).

⁴⁴⁵ See *The al Qaeda – Taliban Connection*.

see the fear of Americans all over the world.”⁴⁴⁶ Afghan terrorists had previously viewed suicide attacks as taboo, but al-Qaeda convinced it that such attacks were religiously permissible.

Al-Qaeda trumpeted that success online, announcing, “While suicide attacks were not accepted in the Afghani culture in the past, they have now become a regular phenomenon!”⁴⁴⁷ With al-Qaeda’s authorization, the number of suicide attacks in Afghanistan increased from one in 2002, two in 2003, and six in 2004 to 21 in 2005, and more than 100 in 2006. Thereafter, suicide bombings remained a cornerstone of the Taliban’s strategy.

1240. As a result, al-Qaeda’s role in that suicide-bombing trend was pivotal and was the but-for cause of each Taliban suicide bomb attack.

1241. Al-Qaeda also authorized the Taliban’s use of IED attacks against Americans in Afghanistan, and bin Laden regularly called for terrorists to attack Americans with IEDs.

2. Al-Qaeda Planned the Attacks that Injured Plaintiffs

1242. Al-Qaeda also planned the Taliban’s terrorist attacks against Americans in Afghanistan. Working through its Syndicate partners and from its safe havens on both sides of the Afghanistan-Pakistan border, al-Qaeda “plan[ned] international as well as regional terrorist attacks, particularly in Afghanistan.”⁴⁴⁸ Two terrorism scholars explained al-Qaeda’s Syndicate-related shuras as follows:

The staying power of al-Qaeda became rooted in its ability to draw from and coordinate with allied groups embedded in multiple networks on both sides of the border. . . . It established a number of shuras to ***coordinate strategy, operations, and tactics*** against the West and regional allied governments. In particular, al-Qaeda fighters have been involved in ***planning and carrying out suicide***

⁴⁴⁶ *Osama bin Laden: Calls for Martyrdom Operations Against US and British Interests* (Apr. 10, 2003) (emphasis added).

⁴⁴⁷ Brian Glyn Williams, *Suicide Bombings in Afghanistan* at 5, *Jane’s Islamic Affairs Analyst* (Sept. 2007).

⁴⁴⁸ *Resilient al-Qaeda* at 3.

attacks, developing improved explosive devices, and helping conduct operations against high-value targets.⁴⁴⁹

1243. Al-Qaeda training provided another key mechanism through which that planning occurred. Before the September 11 attacks, al-Qaeda operated training camps in eastern Afghanistan at the Taliban's request. By 2005 at the latest, al-Qaeda began bringing instructors from Iraq to train the Taliban how to fight Americans. At all relevant times, these al-Qaeda camps trained terrorists in the al-Qaeda signature of turning fertilizer into bombs.

1244. By the mid-2000s, al-Qaeda's partnership with the Haqqani Network had facilitated the emergence of a network of al-Qaeda training camps in North Waziristan, many of which were also affiliated with Sirajuddin Haqqani.⁴⁵⁰

1245. The training continued throughout the relevant timeframe of this case. In 2015, for example, U.S. and Afghan forces raided two al-Qaeda training camps in Kandahar Province – both reportedly “hosted by the Taliban.”⁴⁵¹ One camp was the largest al-Qaeda facility discovered since the September 11 attacks, occupying nearly 30 square miles. On information and belief, this camp trained terrorists in how to make CAN fertilizer bombs and included an on-site al-Qaeda CAN fertilizer bomb factory.

1246. Working jointly with polyterrorist Sirajuddin Haqqani, al-Qaeda specifically planned the Kabul Attack Network's campaign of terror, including its suicide bomber attacks. As two terrorism scholars explained, the “operational and tactical cooperation” provided by

⁴⁴⁹ *Id.* at 3-4.

⁴⁵⁰ Def. Intelligence Agency, *Intelligence Information Report: Location and Activities of the Training Centers Affiliated with the Haqqani Network, Taliban, and al-Qaeda in Northern Waziristan and Future Plans and Activities of Sarajuddin ((Haqqani))* (Apr. 16, 2008) (listing training camps and some of the terrorists there).

⁴⁵¹ Thomas Joscelyn & Bill Roggio, *Trump's Bad Deal With The Taliban*, Politico (Mar. 18, 2019).

al-Qaeda “increased the ability of the Haqqani Network to carry out sophisticated attacks in Kabul,” “through operations [that al-Qaeda] planned together with Sirajuddin Haqqani.”⁴⁵²

1247. Al-Qaeda also planned the Taliban’s attacks by devising the operational scheme for them. Information derived from al-Qaeda and Taliban detainees held at Guantanamo Bay, Cuba (“Gitmo”) corroborates those activities. For example, according to purported Gitmo intelligence files quoted by terrorism experts Bill Roggio and Thomas Joscelyn, one detainee, Abdul Razak, was “a high-level military commander in a newly-conceived ‘unification’ of Al Qaeda, [Hezb-e-Islami Gulbuddin (“HIG”)] and Taliban forces within Afghanistan,” which the groups’ respective leaders conceived during a meeting in Pakistan in early spring 2003.⁴⁵³ Another Gitmo detainee files similarly documented “joint operations meeting[s]” where the participants, which included al Qaeda, Taliban and LT commanders “decided to increase terrorist operations in the Kapisa, Kunar, Laghman, and Nangarhar provinces, including suicide bombings, mines, and assassinations.”⁴⁵⁴ Together, these reports “demonstrate a high degree of collusion between al Qaeda and other terrorist groups” as part of a “jihadist hydra” that shared the “common goal” of seeking to “drive the U.S.-led coalition out of Afghanistan.”⁴⁵⁵

1248. Al-Qaeda also taught the Taliban effective terrorist tradecraft. Through its relationship with al-Qaeda, the Taliban “developed or acquired new commercial communications gear and field equipment,” as well as “good tactical, camouflage, and marksmanship training.”⁴⁵⁶ They also “share[d] communication and transportation routes, coordinate[d] attacks, and even

⁴⁵² *Resilient al-Qaeda* at 9.

⁴⁵³ *The al Qaeda – Taliban Connection*.

⁴⁵⁴ *Id.* (brackets in original).

⁴⁵⁵ *Id.*

⁴⁵⁶ *Id.* at 293.

utilize[d] the same explosive and suicide-bomber networks.”⁴⁵⁷ The Taliban’s (including its Haqqani Network’s) effective terrorist tradecraft was essential to its ability to execute al-Qaeda’s nationwide CAN fertilizer bomb campaign, which depended upon sophisticated logistics, communications, smuggling, storage, and other technical skills that the Taliban only acquired through its relationship with al-Qaeda.

1249. All these activities were part of al-Qaeda’s planning of the Taliban’s CAN fertilizer bomb attacks in Afghanistan. By providing an array of advice, direction, and material support to the Taliban, al-Qaeda was able to use the Taliban for its own jihadist ends. In so doing, al-Qaeda followed its more general practice of planning terrorist attacks whose details it would delegate to local Islamist proxies. As terrorism scholar Thomas Ruttig observed: “Both in Afghanistan and Pakistan, al-Qaeda exploits local conditions by co-opting militant groups with local battle experience.”⁴⁵⁸ Here, its “cooptation” of the Taliban was especially effective.

C. In Furtherance Of The IRGC Conspiracy, Al-Qaeda Committed Terrorist Attacks That Killed And Injured Plaintiffs In Joint Cells With The Taliban, Lashkar-E-Taiba, and Jaish-E-Mohammed

1250. Working together, the Syndicate terrorist groups committed every IED and suicide bomb attack in this case. *See, e.g., e.g., Cabrera* at *1, *40. Consistent with bin Laden’s playbook, al-Qaeda provided the technical expertise, training, ratlines, forward deployed support in Afghanistan, and fundraising support, while the Taliban (including its Haqqani Network) and their Syndicate allies provided training camps, safe houses, front companies to purchase components, and the terrorists to be trained by al-Qaeda to attack Americans in Afghanistan.

⁴⁵⁷ *Resilient al-Qaeda* at 9.

⁴⁵⁸ Thomas Ruttig, *The Other Side* at 22, Afghanistan Analysts Network (July 2009) (“*Ruttig, The Other Side*”).

1251. Al-Qaeda members also committed at least 29 out of the 64 terrorist attacks that killed or injured Plaintiffs and their loved ones alongside the Taliban. In fact, many Syndicate terrorist operatives were “dual-hatted,” meaning that they were both al-Qaeda and Taliban members. *See, e.g., Cabrera* at *8. Those dual-hatted al-Qaeda/Taliban terrorists directly committed many of the attacks that killed and injured Plaintiffs. Examples are set forth below.

1252. **Nangarhar, Nuristan, Kunar and Laghman Provinces (“N2KL”).** In the strategically critical (and contiguous) N2KL Provinces, which were well-known al-Qaeda strongholds, al-Qaeda, the Taliban, and Lashkar-e-Taiba maintained joint cells responsible for anti-American terrorism, each of which executed the Syndicate’s CAN fertilizer bomb campaign in Afghanistan. Al-Qaeda deployed senior operatives to coordinate attacks in N2KL and such al-Qaeda terrorists committed all the attacks in N2KL that killed or injured Plaintiffs or their loved ones alongside the Taliban. *See, e.g., Cabrera* at *14. The dual-hatted al-Qaeda/Taliban polyterrorists who ran these joint cells included:

- (i) **Farouq al-Qahtani**, al-Qaeda’s “emir for eastern Afghanistan” who “supported the Taliban-led insurgency against the Afghan government, US forces and their allies.”⁴⁵⁹
- (ii) **Sakhr al-Taifi**, al-Qaeda’s number two in Afghanistan, who embedded with the Taliban, “coordinate[d] and direct[ed] insurgent attacks against” “coalition troops throughout eastern Afghanistan,” and “supplie[d] weapons and equipment to insurgents.”⁴⁶⁰
- (iii) **Mufti Assad**, an al-Qaeda network and “insurgent leader who controlled al-Qaida terrorists operating in Kunar,” “led dozens of all-Qaida affiliated fighters throughout eastern Afghanistan and coordinated their attacks across the region,” and “was also an explosives expert who” “train[ed] [] insurgents on how to construct and use [IEDs].”⁴⁶¹
- (iv) **Abdallah Umar al-Qurayshi**, a senior al-Qaeda operative who commanded the joint al-Qaeda/Taliban cells operating in Kunar and Nuristan Provinces.

⁴⁵⁹ Thomas Joscelyn, *Pentagon Confirms Death of Senior al Qaeda Leader In Afghanistan*, Long War Journal (Nov. 4, 2016), <https://tinyurl.com/2p859bcj>.

⁴⁶⁰ ISAF, *Morning Operational Update*, Def. Visual Info. Distribution Serv. (May 28, 2012).

⁴⁶¹ ISAF, *Morning Operational Update*, Def. Visual Info. Distribution Serv. (Aug. 5, 2012).

- (v) **Abu Atta al-Kuwaiti**, a senior al-Qaeda explosives expert who coordinated the Nuristan and Kunar Province al-Qaeda/Taliban joint cells' IED and suicide bomb attacks.
- (vi) **Abu Ikhlas al-Masri**, an al-Qaeda commander who helped coordinate al-Qaeda / Taliban attacks in Kunar Province from 2008 until his capture in December 2010.
- (vii) **Sa'ad bin Abi Waqas**, a senior al-Qaeda leader who "coordinated attacks against coalition forces," throughout Kunar Province, "conducted training" and helped terrorists with "weapons procurement."⁴⁶²
- (viii) **Abu Hafs al-Najdi (aka Abdul Ghani)**, a senior al-Qaeda operative who directed al-Qaeda operations in Kunar Province, and was responsible for "planning attacks against" "coalition forces" and "directing suicide-bomb attacks targeting U.S. government officials" that were facilitated by his "network" of Taliban terrorists.⁴⁶³
- (ix) **Fatah Gul**, an al-Qaeda facilitator who "ran terrorist training camps where insurgents learned how to conduct [IED] attacks" in N2KL Provinces.⁴⁶⁴

1253. **Paktika, Paktia, and Khost Provinces ("P2K").** Like its N2KL Provinces, Afghanistan's P2K Provinces (aka Loya Paktia) were a strategically key area that long served as a Haqqani stronghold and "traditional al-Qaeda safe haven[]." ⁴⁶⁵ Al-Qaeda and the Taliban, through the Haqqani Network, maintained joint cells responsible for anti-American terrorism in P2K, each of which executed the Syndicate's CAN fertilizer bomb and suicide campaign in Afghanistan. In addition to **Sirajuddin Haqqani**, *supra*, dual-hatted al-Qaeda/Taliban polyterrorists who ran these P2K-related joint cells included: (i) **Bekkay Harrach (aka al-Hafidh Abu Talha al-Almani)**, a senior member of al-Qaeda's external operations branch, who specifically planned, authorized, and helped commit Haqqani Network attacks while living under the direct protection of Siraj; and (ii) **Khalil al-Rahman Haqqani**, Jalaluddin Haqqani's brother and a dual-hatted al-Qaeda/Taliban terrorist, serving as a "fundraiser, financier, and operational

⁴⁶² ISAF, *Morning Operational Update*, Def. Visual Info. Distribution Serv. (Apr. 16, 2011).

⁴⁶³ U.S. Dep't of Def., *Strike Kills No. 2 Insurgent in Afghanistan* (Apr. 26, 2011).

⁴⁶⁴ ISAF, *Morning Operational Update* (Aug. 5, 2012).

⁴⁶⁵ *Resilient al-Qaeda* at 11-12.

commander” for the Haqqani Network,⁴⁶⁶ as well as an agent who “acted on behalf of al-Qa’ida”⁴⁶⁷ and had “been linked to al-Qa’ida terrorist operations.”⁴⁶⁸

1254. **Kabul and the Kabul Attack Network-Related Provinces.** Kabul City and the strategically critical cluster of provinces around Afghanistan’s capital was the focus of the Kabul Attack Network, where al-Qaeda and the Taliban, maintained joint al-Qaeda/Taliban cells that planned and committed terrorist attacks, each of which executed the Syndicate’s CAN fertilizer bomb and/or suicide attack campaign in Kabul Attack Network-related provinces. Al-Qaeda deployed senior operatives to coordinate attacks in the strategically critical cluster of provinces around the capital city of Kabul, and such al-Qaeda terrorists committed all the attacks in Kabul City and Kabul Attack Network-related areas like Ghazni and Wardak that killed or injured Plaintiffs or their loved ones alongside the Taliban. *See, e.g., Cabrera* at *14. In addition to **Sirajuddin Haqqani**, *supra*, such dual-hatted al-Qaeda/Taliban polyterrorists who ran the cells included **Ahmed Jan Wazir**, a dual-hatted al-Qaeda/Taliban terrorist whom al-Qaeda and the Taliban jointly appointed as commander of their joint cell in Ghazni Province in 2008.

X. THE IRGC-BACKED TALIBAN TERRORIST SYNDICATE IN AFGHANISTAN AND PAKISTAN LED BY AL-QAEDA AND THE TALIBAN KILLED AND INJURED PLAINTIFFS THROUGH TERRORIST ATTACKS FOR WHICH DEFENDANTS PROVIDED SUBSTANTIAL ASSISTANCE

1255. Plaintiffs are American civilians, servicemembers, and contractors serving in Afghanistan, and their family members, who were killed or injured in terrorist attacks committed

⁴⁶⁶ Bill Roggio, *US Designates al Qaeda, Haqqani Network Leaders As Terrorists*, Long War J. (Feb. 9, 2011).

⁴⁶⁷ Press Release, U.S. Dep’t of Treasury, *Treasury Targets The Financial And Support Networks of Al Qa’ida And The Taliban, Haqqani Network Leadership* (Feb. 9, 2011).

⁴⁶⁸ Press Release, U.S. Dep’t of State, *Rewards for Justice - Reward Offers for Information on Haqqani Network Leaders* (Aug. 20, 2014).

by al-Qaeda (a designated FTO at the time), the Taliban, including its Haqqani Network (a designated FTO at the time), Lashkar-e-Taiba (a designated FTO at the time), and Jaysh-e-Mohammed (a designated FTO at the time), all of which collaborated in a terrorist alliance, known as the “Syndicate,” that was funded, armed, and logistically supported by Hezbollah, the Qods Force, and Regular IRGC. For those Plaintiffs below with family members who were injured or died as a result, each Plaintiff has experienced severe mental anguish, emotional pain and suffering, and the loss of their family member’s society, companionship, and counsel.

1256. Hezbollah, the Qods Force, and Regular IRGC provided key aid to the Syndicate from inception through their victory in 2021. Hezbollah, the Qods Force, and Regular IRGC specifically provided al-Qaeda and the Taliban (including its Haqqani Network) weapons, funds, training, logistical support, communications technology, safe haven, and assistance with narcotics trafficking, which raised money for their shared terrorist enterprise against America (i.e., the Conspiracy), which al-Qaeda and the Taliban, including its Haqqani Network, used to aid the terrorists’ ability to execute the attacks that injured Plaintiffs.

1257. The embargoed dual-use American technology – including thousands of secure American smartphones every year – hundreds of millions of U.S. Dollars annually, and vast network of logistical and operational support for the Irancell and TCI fronts that MTN Group, MTN Dubai, ZTE Corporation, Huawei Corporation, and their subsidiary Defendants provided to their counterparties controlled by Hezbollah, the Qods Force, and Regular IRGC flowed through to al-Qaeda, the Taliban (including its Haqqani Network), and their Syndicate allies that committed each attack that injured each Plaintiff through transfers made by Hezbollah, the Qods Force, and Regular IRGC to al-Qaeda and the Taliban (including its Haqqani Network).

1258. On information and belief, each bomb that the Syndicate detonated during each IED attack alleged below was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

1259. Each attack alleged below would have violated the laws of war if these terrorists were subject to them because, *inter alia*, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and each IED's passive detonation system and each suicide bomb attack indiscriminately placed civilians at risk.

A. August 20, 2013 Small Arms Attack in Wardak (George Bannar Jr.)

1260. On August 20, 2013, the Haqqani Network, an FTO, committed a small arms attack in Wardak Province, Afghanistan (the "August 20, 2013 Attack"), which was facilitated by the IRGC's provision of funding, weapons, training, and logistical support to al-Qaeda and the Taliban, including its Haqqani Network. Al-Qaeda planned and authorized the August 20, 2013 Attack.

1261. **Master Sergeant George Bannar Jr.** served in Afghanistan as a member of the U.S. Army. MSG Bannar was injured in the August 20, 2013 Attack. MSG Bannar died on August 20, 2013 as a result of injuries sustained during the attack.

1262. MSG Bannar was a U.S. national at the time of the attack and his death.

1263. Plaintiff Sheila Long is the mother of MSG Bannar and a U.S. national.

1264. As a result of the August 20, 2013 Attack and MSG Bannar's injuries and death, each member of the Bannar Family has experienced severe mental anguish, emotional pain and suffering, and the loss of MSG Bannar's society, companionship, and counsel.

1265. As a result of the August 20, 2013 Attack, MSG Bannar was injured in his person and/or property. The Plaintiff members of the Bannar Family are the survivors and/or heirs of MSG Bannar and are entitled to recover for the damages MSG Bannar sustained.

B. January 20, 2014 Small Arms Attack in Kandahar (Edward Balli)

1266. On January 20, 2014, the Taliban committed a small arms attack in Kandahar Province, Afghanistan (the “January 20, 2014 Attack”), which was facilitated by the IRGC’s provision of funding, weapons, training, and logistical support to al-Qaeda and the Taliban. Al-Qaeda planned and authorized the January 20, 2014 Attack.

1267. **Chief Warrant Officer 2 Edward Balli** served in Afghanistan as a member of the U.S. Army. CW2 Balli was injured in the January 20, 2014 Attack. CW2 Balli died on January 20, 2014 as a result of injuries sustained during the attack.

1268. CW2 Balli was a U.S. national at the time of the attack and his death.

1269. Plaintiff Michael Donios is the son of CW2 Balli and a U.S. national.

1270. As a result of the January 20, 2014 Attack and CW2 Balli’s injuries and death, each member of the Balli Family has experienced severe mental anguish, emotional pain and suffering, and the loss of CW2 Balli’s society, companionship, and counsel.

1271. As a result of the January 20, 2014 Attack, CW2 Balli was injured in his person and/or property. The Plaintiff members of the Balli Family are the survivors and/or heirs of CW2 Balli and are entitled to recover for the damages CW2 Balli sustained.

C. June 2, 2014 Small Arms Attack in Nangarhar (Jason Jones)

1272. On June 2, 2014, al-Qaeda, an FTO, and the Taliban, acting together as a joint al-Qaeda/Taliban cell, committed a small arms attack in Nangarhar Province, Afghanistan (the “June 2, 2014 Attack”), which was facilitated by the IRGC’s provision of funding, weapons,

training, and logistical support to al-Qaeda and the Taliban. Al-Qaeda planned and authorized the June 2, 2014 Attack.

1273. **Captain Jason Jones** served in Afghanistan as a member of the U.S. Army. CPT Jones was injured in the June 2, 2014 Attack. CPT Jones died on June 2, 2014 as a result of injuries sustained during the attack.

1274. CPT Jones was a U.S. national at the time of the attack and his death.

1275. Plaintiff Joseph Jones Jr. is the father of CPT Jones and a U.S. national.

1276. As a result of the June 2, 2014 Attack and CPT Jones's injuries and death, each member of the Jones Family has experienced severe mental anguish, emotional pain and suffering, and the loss of CPT Jones's society, companionship, and counsel.

1277. As a result of the June 2, 2014 Attack, CPT Jones was injured in his person and/or property. The Plaintiff members of the Jones Family are the survivors and/or heirs of CPT Jones and are entitled to recover for the damages CPT Jones sustained.

XI. THE IRGC'S TERRORIST PROXIES COMMITTED, PLANNED, AND AUTHORIZED THE ATTACK THAT INJURED PLAINTIFF MATTHEW SCHRIER IN SYRIA

1278. The IRGC used its resources to provide al-Qaeda, AQI, and ANF funds, operational support, logistical support, communications technology, and safe haven, which raised money for their shared terrorist objectives against America. Al-Qaeda, AQI, and ANF, used these resources to commit the attacks that injured Plaintiff Matthew Schrier.

1279. Plaintiff Matthew Schrier was an American photojournalist who was injured in a hostage-taking attack committed by al-Nusra Front that was funded, armed, and logistically supported by the IRGC, including the IRGC-QF.

1280. On December 31, 2012, al-Nusra Front kidnapped Mr. Schrier in Aleppo, Syria. ANF held Mr. Schrier hostage for 211 days, during which ANF tortured him, before he escaped

to his freedom on July 29, 2013. Al-Qaeda and AQI planned and authorized ANF's attack against Mr. Schrier.

1281. Mr. Schrier's kidnapping, subsequent confinement, and torture would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the terrorists kidnapped and murdered an unarmed civilian who was not engaged in hostilities.

1282. Mr. Schrier was a U.S. national throughout the attack and remains one today.

1283. As a result of his kidnapping and torture, Mr. Schrier has experienced severe mental anguish, emotional pain and suffering, and was injured in his person and/or property.

CLAIMS FOR RELIEF

COUNT ONE: VIOLATION OF THE ANTI-TERRORISM ACT, 18 U.S.C. § 2333(d) **[All Defendants: Aiding-And-Abetting Liability, Attack Predicate]**

1284. Plaintiffs incorporate their factual allegations above.

1285. The terrorist attacks that killed or injured Plaintiffs or their family members were acts of international terrorism against Americans in Afghanistan or Syria were: (i) committed by joint cells comprised of al-Qaeda (a designated FTO since 1999) and the Taliban⁴⁶⁹ (a designated SDGT at all times), including its Haqqani Network (a designated SDGT after 2001 and a designated FTO after September 19, 2012), with the material support of the IRGC,⁴⁷⁰ including Hezbollah (a designated FTO since 1997) and the Qods Force (a designated SDGT after October 25, 2007), which attacks were planned and/or authorized by al-Qaeda; (ii) committed by the

⁴⁶⁹ In each Count in this Complaint, any reference to "Taliban" is inclusive of the Haqqani Network, which is a part of the Taliban.

⁴⁷⁰ In each Count in this Complaint, any reference to "IRGC" is inclusive of Hezbollah, the Qods Force, and Regular IRGC, all of which are constituent parts of the IRGC.

Taliban, including its Haqqani Network, with the material support of the IRGC, including Hezbollah and the Qods Force, which attacks were planned and/or authorized by al-Qaeda; or (iii) committed by ANF (a designated FTO since December 2004) and planned and/or authorized by al-Qaeda (a designated FTO at all times) and/or al-Qaeda-in-Iraq (a designated FTO since December 2004).

1286. The terrorist attacks in Afghanistan committed by al-Qaeda and/or the Taliban, with the material support of the IRGC, which killed or injured all Afghanistan Plaintiffs and their family members, and the attack in Syria committed by ANF, with the material support of the IRGC, which injured Plaintiff Matthew Schrier, were violent acts and acts dangerous to human life that violated the criminal laws of the United States and many States, or would have violated those laws had they been committed within the jurisdiction of the United States or of the States. In particular, each attack constituted one or more of murder, attempted murder, conspiracy to murder, kidnapping, and arson, in violation of state law; and the destruction of U.S. property by fire or explosive, conspiracy to murder in a foreign country, killing and attempted killing of U.S. employees performing official duties, hostage taking, damaging U.S. government property, killing U.S. nationals abroad, use of weapons of mass destruction, commission of acts of terrorism transcending national boundaries, and bombing places of public use, in violation of 18 U.S.C. §§ 844(f)(2) or (3), 956(a)(1), 1114, 1203, 1361, 2332, 2332a, 2332b, and 2332f, respectively.

1287. The terrorist attacks in Afghanistan committed by al-Qaeda and/or the Taliban, with the material support of the IRGC, which killed or injured all Afghanistan Plaintiffs and their family members, and the terrorist attack in Syria committed by ANF, which injured Plaintiff Matthew Schrier, appear to have been intended (a) to intimidate or coerce the civilian

populations of Afghanistan, Iraq, Syria, the United States, and other Coalition nations, (b) to influence the policy of the U.S., Afghan, Iraqi, Syrian and other governments by intimidation and coercion, and (c) to affect the conduct of the U.S., Afghan, Iraqi, Syrian, and other governments by mass destruction, assassination, and kidnapping.

1288. The terrorist attacks in Afghanistan committed by al-Qaeda and/or the Taliban, with the material support of the IRGC, and the terrorist attack in Syria committed by ANF, with the material support of the IRGC, occurred primarily outside the territorial jurisdiction of the United States.

1289. Each of MTN Irancell, MTN Group, MTN Dubai, ZTE Corp., ZTE USA, ZTE TX, Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom aided and abetted and knowingly provided substantial assistance to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, the Taliban, including its Haqqani Network, AQI, and ANF – and aided and abetted and knowingly provided substantial assistance to the al-Qaeda and/or Taliban attacks that injured the Afghanistan Plaintiffs, and the ANF attack that injured Plaintiff Matthew Schrier – by providing funds to known IRGC fronts and technical help to Hezbollah, the Qods Force, and Regular IRGC that aided those attacks, and by making cash and free goods protection payments to the Taliban, including its Haqqani Network.

1290. MTN, including but not limited to in coordination with MTN Dubai, also aided and abetted and knowingly provided substantial assistance to Hezbollah, the Qods Force, and Regular IRGC – and aided and abetted and knowingly provided substantial assistance to the IRGC's proxy attacks on the Afghanistan Plaintiffs committed by al-Qaeda and/or the Taliban, and to the IRGC's proxy attack on Plaintiff Matthew Schrier committed by AQI, including al-Nusra Front, in Syria – by serving as the joint venture partner of Hezbollah, the Qods Force, and

Regular IRGC and generating millions of dollars in annual cash flow for Hezbollah, the Qods Force, and Regular IRGC to further the IRGC's support for proxy attacks by al-Qaeda and/or the Taliban against Americans in Afghanistan, and by AQI, including al-Nusra Front, in Iraq and Syria.

1291. ZTE, including but not limited to in coordination with ZTE USA and ZTE TX, aided and abetted and knowingly provided substantial assistance to Hezbollah, the Qods Force, and Regular IRGC – and aided and abetted and knowingly provided substantial assistance to the IRGC's proxy attacks on the Afghanistan Plaintiffs committed by al-Qaeda and/or the Taliban in Afghanistan, and on Plaintiff Matthew Schrier committed by al-Nusra Front in Syria – by contracting with TCI to modernize the IRGC-controlled Iranian cellular and landline communications systems, thereby generating substantial revenue for Hezbollah, the Qods Force, and Regular IRGC and provided U.S.-origin technology to the IRGC, which the IRGC flowed through to al-Qaeda and the Taliban, including its Haqqani Network, in Afghanistan, all of which al-Qaeda and the Taliban, including its Haqqani Network, used in furtherance of al-Qaeda's and the Taliban's, including the Haqqani Network's, shared terrorist attacks against Americans in Afghanistan, and which the IRGC also flowed through to al-Qaeda-in-Iraq, including al-Nusra Front, in Iraq and Syria, all of which al-Qaeda-in-Iraq and al-Nusra Front used in furtherance of ANF's attacks against Americans in Syria.

1292. Huawei, including but not limited to and in coordination with Skycom, Huawei USA, Huawei Device USA, and Futurewei, aided and abetted and knowingly provided substantial assistance to Hezbollah, the Qods Force, and Regular IRGC – and aided and abetted and knowingly provided substantial assistance to the IRGC's proxy attacks on the Afghanistan Plaintiffs committed by al-Qaeda and/or the Taliban in Afghanistan, and on Plaintiff Matthew

Schrier committed by ANF in Syria – by contracting with TCI to modernize the IRGC-controlled Iranian cellular and landline communications systems, thereby generating substantial revenue for Hezbollah, the Qods Force, and Regular IRGC and illegally provided U.S.-origin technology to Hezbollah, the Qods Force, and Regular IRGC, which the IRGC flowed through to al-Qaeda and the Taliban, including its Haqqani Network, in Afghanistan, all of which al-Qaeda and the Taliban, including its Haqqani Network, used in furtherance of al-Qaeda's and the Taliban's, including the Haqqani Network's, shared terrorist attacks against Americans in Afghanistan, and which the IRGC also flowed through to al-Qaeda-in-Iraq, including al-Nusra Front, in Iraq and Syria, all of which al-Qaeda-in-Iraq and al-Nusra Front used in furtherance of ANF's attacks against Americans in Syria.

1293. The attacks that killed or injured Plaintiffs and their family members were all jointly committed, as well as planned and authorized, by al-Qaeda, which the United States has designated as an FTO under 8 U.S.C. § 1189 since 1999, and/or al-Qaeda-in-Iraq (including al-Nusra Front), which the United States has designated as an FTO since 2004.

1294. The Afghanistan Plaintiffs are U.S. nationals who were injured in their persons, properties, and/or businesses by reason of the terrorist attacks committed by al-Qaeda and/or the Taliban in Afghanistan. Plaintiff Matthew Schrier is a U.S. national who was injured in his person, property, and/or business by reason of the terrorist attacks committed by al-Qaeda-in-Iraq and al-Nusra Front in Syria. Plaintiffs suffered economic, physical, and emotional injuries proximately caused by the attacks; are survivors and/or heirs of U.S. nationals who suffered such injuries; or both.

1295. As a result of Defendants' liability under 18 U.S.C. § 2333(d), Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

COUNT TWO: VIOLATION OF THE ANTI-TERRORISM ACT, 18 U.S.C. § 2333(d)
[All Defendants: Conspiracy Liability; Attack Predicate]

1296. The Afghanistan Plaintiffs incorporate their factual allegations above.

1297. Each of MTN Irancell, MTN Group, MTN Dubai, ZTE Corp., ZTE USA, ZTE TX, Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom entered into the Conspiracy with the “Iranian Shareholders,” and one another, including but not limited to the Bonyad Mostazafan, IEI, TCI (including MCI), and Exit40, all of whom were fronts for the IRGC (collectively, “IRGC Fronts”), including its Hezbollah Division and Qods Force, as well as the IRGC’s terrorist co-conspirators in Afghanistan, al-Qaeda and the Taliban (including its Haqqani Network), to join the IRGC’s terrorist financing and logistics campaign.

1298. Each of MTN Irancell, MTN Group, MTN Dubai, ZTE Corp., ZTE USA, ZTE TX, Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom furthered the Conspiracy through their knowing direct and/or indirect participation in the IRGC’s broad, coordinated, global campaign to source embargoed American technologies to aid the Conspiracy’s terrorist enterprise, including but not limited to, secure American mobile phones and computer network technologies.

1299. Given the illegal nature of the market for embargoed American technologies, each Defendant’s choice to further the Conspiracy by paying inflated prices above even the normal “going rate” for black market phones furthered the terrorist enterprise by substantially growing the black market for such technologies through the power of supply and demand. Every time each Defendant flooded the zone by promising to outspend every other black market participant, Defendants swelled the ranks of their co-conspirator tech resellers on the supply side in the U.S.

1300. Each of MTN Group, MTN Irancell, MTN Dubai, ZTE Corp., ZTE USA, ZTE TX, Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom specifically

intended to grow the overall global market for illicit American-manufactured mobile phones that were originally sold in a U.S. marketplace because they shared the goal of the Conspiracy, which was to finance, arm, and logistically support Hezbollah, the Qods Force, and Regular IRGC.

1301. Each of MTN Group, MTN Irancell, MTN Dubai, ZTE Corp., ZTE USA, ZTE TX, Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom was one in spirit with the terrorists, including, but not limited to, Hezbollah, the Qods Force, and Regular IRGC, as well as IRGC Syndicate Terrorist Proxies al-Qaeda and the Taliban, including its Haqqani Network, all of whom received weapons, funding, and training from the IRGC.

1302. Each Defendant hoped for the IRGC, including, but not limited to, its Hezbollah Division and Qods Force, to achieve the object of the Conspiracy and force the United States to withdraw from Afghanistan, Iraq, and the rest of the Middle East. Defendants knew that Hezbollah, the Qods Force, and Regular IRGC were extremely lucrative customers and generated billions of dollars in profits for each Defendant, and Defendants wanted to see the Conspiracy succeed because they calculated they would make more money if the terrorist campaigns in Afghanistan, Iraq, and the rest of the Middle East forced the U.S. out.

1303. Defendants ZTE and Huawei also supported the object of the Conspiracy because it furthered the hostile security strategy of the Chinese Communist Party to force the United States out of Iraq, Afghanistan, and the rest of the Middle East by aiding the terrorist groups targeting Americans throughout the region.

1304. Each Defendant furthered the Conspiracy by directly aiding the growth of the terrorists' supply chain through the foreseeable, inevitable, and obvious result that Defendants knew – and intended – would occur when they paid above-black market prices for illicit American technologies. Defendants knew that their deals would strengthen the terrorists' illicit

technological supply chain by exploding the demand for suppliers, and specifically intended for this consequence to occur to benefit Hezbollah, the Qods Force, and Regular IRGC. As a result, each Defendant furthered the Conspiracy by increasing the total volume of illicit American mobile phones and computer network technologies specifically available for, and intended to be purchased by, the agents, operatives, cut-outs, or corporate fronts acting on behalf of Hezbollah, and the Qods Force, all of whom received substantially more illicit technologies than would otherwise have been the case if Defendants had not participated in the black market.

1305. Each supplier Defendant – MTN Group, MTN Dubai, ZTE Corp. and Huawei Co. – furthered the Conspiracy by publicly denying the existence of their secret deal to aid the “security” agenda of MTN Irancell’s and TCI’s Iranian Shareholders, i.e., Hezbollah, the Qods Force, and Regular IRGC.

1306. Each manufacturer Defendant – ZTE (USA) Inc., ZTE (TX) Inc., Huawei Technologies Co., Ltd., Huawei Technologies USA Inc., and Huawei Device USA Inc., – furthered the Conspiracy by, among other things: (1) knowingly supplying state-of-the-art American technology while knowing that such technology was being transferred pursuant to deals that were designed to flow the technology through to Hezbollah, the Qods Force, and Regular IRGC; and (2) on information and belief, subsidizing the bribes that ZTE Corp. paid to IRGC officials to secure ZTE’s business with the IRGC’s fronts.

1307. ZTE (USA) Inc. and ZTE (TX) Inc. also furthered the Conspiracy by successfully interfering with whistleblower activity, which, on information and belief, materially delayed the disclosure of the fraud, and further concealed the scheme, causing substantial additional value to flow to the terrorists.

1308. ZTE (USA) Inc.'s and ZTE (TX) Inc.'s retaliation against one or more whistleblowers was an act in furtherance of the Conspiracy because it was intended to deter their future employees, officers, attorneys, or agents from alerting authorities about other potential acts that would destroy the effectiveness of the Conspirators to continue to access the ZTE (USA) Inc. and ZTE (TX) Inc. technology upon which they relied.

1309. MTN Group, MTN Dubai, ZTE, and Huawei agreed to further this Conspiracy by assisting the IRGC Fronts to move large sums of money (primarily in U.S. dollars) through the international financial system (and particularly the United States) undetected.

1310. MTN Group, MTN Dubai, ZTE, and Huawei agreed to further this Conspiracy by each assisting the IRGC Fronts to move tens of thousands of critical items of embargoed American technologies specifically identified by Hezbollah and the Qods Force as necessary to the success of the Conspiracy, through the covert purchase of American-made technologies in U.S. markets, in transactions that were denominated in U.S. Dollars, in sums of money (primarily in U.S. dollars) through the international financial system (and particularly the U.S.) undetected.

1311. Hezbollah, the Qods Force, and Regular IRGC conspired with IRGC Syndicate Terrorist Proxies in Afghanistan (al-Qaeda and the Taliban, including its Haqqani Network) to facilitate terrorist attacks targeting Americans in Afghanistan and Iraq, among other places, for the purpose of targeting U.S. citizens and institutions and affecting the policies of the U.S. government.

1312. Each Defendant knew that the objective of the IRGC Conspiracy between these sophisticated terrorist organizations and the other Defendants was to facilitate terrorist attacks against Americans in Afghanistan, Iraq, Syria, Yemen, Israel, and Europe. This includes the

attacks at issue in this case that were planned, authorized, or executed by designated FTOs and that killed or injured the Afghanistan Plaintiffs and their family members.

1313. These attacks were a foreseeable act in furtherance of this IRGC Conspiracy that caused the Afghanistan Plaintiffs' injuries.

1314. The attacks that killed or injured the Afghanistan Plaintiffs and their family members were all jointly committed, as well as planned and authorized, by al-Qaeda, which the United States has designated as an FTO under 8 U.S.C. § 1189 since 1999.

1315. The Afghanistan Plaintiffs are U.S. nationals who were injured in their persons, properties, and/or businesses by reason of the terrorist attacks committed by al-Qaeda and/or the Taliban, including its Haqqani Network. The Afghanistan Plaintiffs suffered economic, physical, and emotional injuries proximately caused by the attacks; are survivors and/or heirs of U.S. nationals who suffered such injuries; or both.

1316. As a result of Defendants' liability under 18 U.S.C. § 2333(d), the Afghanistan Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

COUNT THREE: VIOLATION OF THE ANTI-TERRORISM ACT, 18 U.S.C. § 2333(d)
[All Defendants: Aiding-and-Abetting Liability, RICO predicate]

1317. Plaintiffs incorporate their factual allegations above.

1318. From at least 2007 through the present, IRGC terrorists from Hezbollah, the Qods Force, and Regular IRGC, and al-Qaeda conspired with Mullah Omar, Sirajuddin Haqqani, and others to conduct and maintain the Taliban as a terrorist enterprise capable of carrying out sophisticated attacks on American targets in Afghanistan. Throughout that time, the Taliban was a group of associated individuals that functioned as a continuing unit, and the Taliban's express

purpose at all times included violence against, and the expulsion of, Americans in Afghanistan. The Taliban engaged in, and its activities affected, foreign commerce.

1319. From at least 2005 through the present, terrorists from Hezbollah, the Qods Force, and Regular IRGC, aided al-Qaeda and the Taliban as the Taliban conspired with Mullah Omar, Sirajuddin Haqqani, and others to conduct and maintain the Taliban as a terrorist enterprise capable of: (1) carrying out sophisticated attacks on American targets in Afghanistan; and (2) aiding the Taliban's co-conspirators, the IRGC (including Hezbollah and the Qods Force) fund attacks on Americans in Iraq and elsewhere in the Middle East through the Taliban's assistance to Hezbollah, the Qods Force, and Regular IRGC, to profit from shared narcotrafficking, money laundering, and arms supply activities, all of which were illegal. Throughout that time, the IRGC, inclusive of its Hezbollah Division and Qods Force, al-Qaeda, and the Taliban, inclusive of its Haqqani Network, was a group of associated individuals that functioned as a continuing unit, and the IRGC's, including Hezbollah's and the Qods Force's, al-Qaeda's, and the Taliban's, including the Haqqani Network's, express purpose at all times included the sustainment and propagation of violence against, and the expulsion of, Americans in Afghanistan and the broader Middle East by one or more of the following members of the Conspiracy: (i) Hezbollah, the Qods Force, and Regular IRGC, and the Iranian Shareholders who own or control the fronts and/or covers associated with Hezbollah, the Qods Force, and Regular IRGC; (ii) MTN Irancell; (3) Telecommunications Company of Iran; (4) Exit40; (5) al-Qaeda; (6) the Taliban; and (7) al-Qaeda-in-Iraq (including ANF). The Taliban engaged in, and its activities affected, foreign commerce.

1320. From at least 2007 through the present, the IRGC, Mullah Omar, Sirajuddin Haqqani and other terrorists employed by or associated with the Taliban and al-Qaeda

(including, without limitation, Jalaluddin Haqqani and other terrorists described in this Complaint) have maintained interests in and conducted the affairs of the Taliban as an enterprise by engaging in a campaign to expel Americans from Afghanistan through crime and anti-American violence (the “IRGC-Taliban-al-Qaeda Campaign”).

1321. Specifically, Mullah Omar, Sirajuddin Haqqani, and other terrorists employed by or associated with the Taliban and al-Qaeda conducted and participated in the conduct of the Taliban’s affairs (and conspired to do so) through a pattern of racketeering activity involving crimes that include murder, attempted murder, conspiracy to murder, kidnapping, and arson, in violation of state law, and the destruction of U.S. property by fire or explosive, conspiracy to murder in a foreign country, killing and attempted killing U.S. employees performing official duties, hostage taking, damaging U.S. government property, killing U.S. nationals abroad, use of weapons of mass destruction, commission of acts of terrorism transcending national boundaries, bombing places of public use, financing terrorism, and receiving training from an FTO, in violation of 18 U.S.C. §§ 844(f)(2) or (3), 956(a)(1), 1114, 1203, 1361, 2332, 2332a, 2332b, 2332f, 2339C(a)(1)(B), and 2339D, respectively. The same terrorists also maintained interests in and control of the Taliban (and conspired to do so) through this pattern of racketeering activity.

1322. The IRGC-Taliban-al-Qaeda Campaign was an act of international terrorism. It was a violent act that was dangerous to human life and that violated the criminal laws of the United States prohibiting the conduct or participation in the conduct of an enterprise’s affairs through a pattern of racketeering activity, 18 U.S.C. § 1962(c); the maintenance of an interest in or control of an enterprise through a pattern of racketeering activity, 18 U.S.C. § 1962(b); and conspiring to do either of these acts, 18 U.S.C. § 1962(d); or would have violated these prohibitions had it been conducted within the jurisdiction of the United States. The IRGC-

Taliban-al-Qaeda Campaign appears to have been intended (a) to intimidate or coerce the civilian populations of Afghanistan, the United States, and other Coalition nations, (b) to influence the policy of the U.S., Afghan, and other Coalition governments by intimidation and coercion, and (c) to affect the conduct of the U.S., Afghan, and other Coalition governments by mass destruction, assassination, and kidnapping.

1323. The IRGC-Taliban-al-Qaeda Campaign occurred primarily outside the territorial jurisdiction of the United States.

1324. Plaintiffs are U.S. nationals who were injured in their persons, properties, and/or businesses by reason of the IRGC-Taliban-al-Qaeda Campaign. Specifically, the attacks that injured Plaintiffs were part of the pattern of racketeering activity through which the IRGC, Mullah Omar, Sirajuddin Haqqani, and other terrorists associated with the Taliban and al-Qaeda conducted the affairs of, participated in conducting the affairs of, and maintained an interest in or control of the Taliban. Plaintiffs suffered economic, physical, and emotional injuries proximately caused by the IRGC-Taliban-al-Qaeda Campaign; are the survivors and/or heirs of U.S. nationals who suffered such injuries; or both.

1325. Defendants aided and abetted and knowingly provided substantial assistance to Hezbollah, the Qods Force, the Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, which flowed through to the IRGC-Taliban-al-Qaeda Campaign. Defendants did so by making payments to the IRGC that indirectly financed the Taliban's terrorist attacks, and, by authorizing, paying, and/or facilitating millions in annual protection payments to the Taliban, including its Haqqani Network, in cash and "free goods" every year since on or about 2008. MTN Group further aided the Taliban, including the Haqqani Network, by deactivating its transmission masts to assist the Taliban's counterintelligence activities and undermine U.S.

counterinsurgency efforts in Afghanistan. On information and belief, MTN Group coordinated its towers shutdowns with the Taliban, including its Haqqani Network.

1326. The IRGC-Taliban-al-Qaeda Campaign was committed, planned, and/or authorized by Hezbollah, al-Qaeda, and the Haqqani Network, each of which the United States has designated as an FTO under 8 U.S.C. § 1189 since (in 1997, 1999, and 2012, respectively).

1327. As a result of Defendants' liability under 18 U.S.C. § 2333(d), Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

JURY DEMAND

1328. In accordance with Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury on all issues so triable.

PRAYER FOR RELIEF

1329. Plaintiffs request that the Court:

- (a) Enter judgment against Defendants finding them jointly and severally liable under the Anti-Terrorism Act, 18 U.S.C. § 2333;
- (b) Award Plaintiffs compensatory and punitive damages to the maximum extent permitted by law, and treble any compensatory damages awarded under the Anti-Terrorism Act pursuant to 18 U.S.C. § 2333(a);
- (c) Award Plaintiffs their attorney's fees and costs incurred in this action, pursuant to 18 U.S.C. § 2333(a);
- (d) Award Plaintiffs prejudgment interest; and
- (e) Award Plaintiffs any such further relief the Court deems just and proper.

Dated: July 28, 2023

Respectfully submitted,

/s/ Eli J. Kay-Oliphant

Eli J. Kay-Oliphant

Geoffrey P. Eaton

Tejinder Singh

Ryan R. Sparacino

Shuman Sohrn

SPARACINO PLLC

1920 L Street, NW, Suite 835

Washington, D.C. 20036

Tel: (202) 629-3530

eli.kay-oliphant@sparacinopllc.com

geoff.eaton@sparacinopllc.com

tejinder.singh@sparacinopllc.com

ryan.sparacino@sparacinopllc.com

shuman.sohn@sparacinopllc.com

Counsel for Plaintiffs